SERA 28
SESSION EUROPEENNE DES RESPONSABLES D’ARMEMENT
REPORTS

INSTITUT DES HAUTES ETUDES DE DEFENSE NATIONALE
Hybrid warfare: which European response

This document compiles the reports drafted in 2016 by the 28th SERA auditors on the general theme “Hybrid warfare: which European response” and its subthemes.

Views and recommendations expressed in this document are those of the committee’s members. In any case, this content reflects neither national policies of any SERA nation, nor positions of any company.

Copying, reproductions, modifications, distribution of any or the contents of this document without prior written consent of IHEDN is strictly prohibited.
I am pleased to address my warmest thanks to the editors of these reports, the 28th “Session européenne des responsables d'armement” auditors and to the involved councilors, for the work carried out throughout this year 2016.

The reports published in this collection are the result, of more than 4 weeks of exchanges and intense discussions in France, Austria and in Sweden.

It demonstrates in concrete terms what Sera seeks to promote: building and federating year after year a community of civil and military executives, from the public and the private sector, aware of the European challenges in the field of armaments and more widely Defence; a network able to work together beyond origins and cultures and build the Europe of tomorrow.

I wish you a fruitful career. I am convinced that we will have the opportunity to meet each other’s in the future.

Sincerely

Major General Daniel Argenson
IHEDN Deputy Director
Armament and Defence Economics advisor
Chairman of the Sera Council of Studies
General SERA presentation

European initiative under the responsibility of the IHEDN, the French "Institut des hautes études de defense nationale", the "session européenne des responsables d’armement" aims to broaden the links between European nations which are planning to co-operate on military procurement programmes since 1989.

The SERA provides senior managers involved in defence equipment matters and in European collaboration with an environment for training and reflection, meetings and uninhibited discussion with the aim of strengthening the European outlook in matters concerning defence and defence equipment and to improve mutual understanding between partners.

This training is provided over 4 weeks, distributed over 5 months between February and June, in France and in two other European countries.

It relies on an original and interactive method built around a group of activities linked to a central theme:

- **Conferences** intended to supply information to the auditors, followed by an exchange of opinions with the speaker.
- **Visits** which give an insight into certain aspects of the defence industry and the organization of the armed forces.
- **Committee work** where each committee (groups of 10 people from different nationalities) is in charge of studying a defined subject whose conclusions are presented at the end of the session in June.
SUMMARY

6
COMMITTEE #1
Hybrid Warfare Unmanned Platforms and Combatant Enhancement New Strategic Challenges for the EU?

30
COMMITTEE #2
Deception, Information and Cyber Warfare: how could Europe approach hybrid warfare levers to her advantage?

77
COMMITTEE #3
How can the EU/Europe/European industry support maintaining and/or reshabing EDTIB for an age of the hybrid warfare?

93
COMMITTEE #4
Trans-Atlantic and international armaments cooperation: risks, opportunities and security issues

109
COMMITTEE #5
European Defence Research: how to cope with hybrid threats and new challenges in 21st century “warfare”?

138
COMMITTEE #6
European Defence Cooperation and Procurement Strategies for the 21st Century: securing best value from Dual Use/Commercial off the Shelf (COTS) and/or Tailored High Tech applications
Committee 1

Hybrid Warfare Unmanned Platforms and Combatant Enhancement
New Strategic Challenges for the EU?

Pilots: Jean-François COUTRIS, Bernard CLERMONT

Members of the Committee

Klaus KUPZIK
Henrik MESSEL (Chairman)
Jarmo VINKVIST
Denis LIZANDIER
Marco GENTILE
Steffen EVJU
Matthijs DE HAAN
Jonathan PARR (Secretary)
Max OBRIST
Artur PLOKSTO
Introduction / definition "hybrid warfare"

The combination of conventional and irregular methods is not new and has been used throughout history e.g. American Revolution when a combination of Washington’s Continental Army worked alongside militia forces. Similarly, in the Napoleonic Wars, British regulars cooperated with Spanish guerrillas. Fast forward and by the end of the Cold War a unipolar system was created with a dominating American military power. Whilst this reduced the potential for traditional conflicts, regional conflicts and threats have still occurred where the conventional military’s structural weaknesses have been highlighted and exploited.

This has been compounded by the increasing sophistication and lethality of non-state actors. These actors are well armed with technologically advanced weapons that are now available at affordable prices. Similarly, commercial technologies such as cell phones and digital networks provide capabilities that enhance non-state actors’ operations.

Defining hybrid warfare is a real challenge. Hybrid warfare continues to be used to express a multitude of concepts. A google search will provide at least 731,000 hits. By examining a variety of definitions from respected institutions Committee 1 has arrived at an appropriate definition in which the question we have been tasked to answer can be considered.

Wikipedia defines Hybrid Warfare as:

“A military strategy that blends conventional warfare, irregular warfare and cyber-warfare. By combining kinetic operations with subversive efforts, the aggressor intends to avoid attribution or retribution.

There are some pertinent aspects to this definition that will be addressed in more detail:

A non-standard, complex, and fluid adversary. A hybrid adversary can be a state or non-state. For example, in the Israel–Hezbollah War and the Syrian Civil War the main adversaries are non-state entities within the state system. These non-state actors can act as proxies for countries but can also have independent agendas. For example, Iran is a sponsor of Hezbollah but it was Hezbollah’s, not Iran’s, agenda that resulted in the kidnapping of Israeli troops that led to the Israel–Hezbollah war. On the other hand, Russian involvement in Ukraine can be described as a traditional state actor waging a hybrid war (in addition to using a local hybrid proxy). Note that Russia denies involvement in the Ukraine conflict.

A hybrid adversary uses a combination of conventional and irregular methods. Methods and tactics include conventional capabilities, irregular tactics, irregular formations, terrorist acts, indiscriminate violence, and criminal activity. A hybrid adversary also uses clandestine actions to avoid attribution or retribution. These methods are used simultaneously across the spectrum of conflict with a unified strategy. A current example is the Islamic State’s transnational aspirations, blended tactics, structured formations, and use of terror as part of their arsenal.
A hybrid adversary is flexible and adapts quickly. For example, the Islamic State’s response to the U.S. aerial bombing campaign was to quickly reduce the use of checkpoints, large convoys, and cell phones. IS militants also dispersed among the civilian population with the full knowledge that civilian collateral damage from airstrikes can be used as an effective recruiting tool.

A hybrid adversary uses advanced weapons systems and other disruptive technologies. These weapons can be now bought at affordable prices on the black market. Many such weapons have fallen into the hands of criminals or terrorists as a result of failed states where official stocks have been looted. In 2006, Hezbollah was armed with high-tech weaponry, such as precision guided missiles, that were once the monopoly of nation-states. Hezbollah’s forces shot down Israeli helicopters, severely damaged a patrol boat with an anti-ship missile and destroyed heavily armored tanks by firing guided missiles from hidden bunkers. The organization also used aerial drones to gather intelligence, communicated via encrypted cell phones and watched Israeli troop movements using thermal night-vision equipment.

Use of mass communication for propaganda. The growth of mass communication networks offers powerful propaganda and recruiting tools on a global scale. Acts of terror can be orchestrated from thousands of miles away. An individual via the internet can be radicalized, recruited, trained, financed and directed.

A hybrid war takes place on three distinct battlefields: the conventional battlefield, within the indigenous population of the conflict zone, and finally the wider international community. Operational definitions encompass many of the aspects that were outlined above. For example:

✓ The U.S. Army Chief of Staff defined a hybrid threat in 2008 as an adversary that incorporates “diverse and dynamic combinations of conventional, irregular, terrorist and criminal capabilities.”

✓ The United States’ Joint Forces Command defines a hybrid threat as, “any adversary that simultaneously and adaptively employs a tailored mix of conventional, irregular, terrorism and criminal means or activities in the operational battle space. Rather than a single entity, a hybrid threat or challenger may be a combination of state and non-state actors.”

✓ The U.S. Army defined a hybrid threat in 2011 as “the diverse and dynamic combination of regular forces, irregular forces, criminal elements, or a combination of these forces and elements all unified to achieve mutually benefiting effects.”

✓ NATO uses the term to describe “adversaries with the ability to simultaneously employ conventional and non-conventional means adaptively in pursuit of their objectives.”

Of all the definitions or statement made on hybrid warfare discovered during our research that the Department of Defence (DOD) had probably the most useful and widely agreed statement within our committee’s discussions:

✓ We have not officially defined “hybrid warfare" at this time and have no plans to do so because the DOD does not consider it a new form of warfare.

✓ Officials from the majority of organizations that the DoD visited agreed that “hybrid warfare” encompasses all elements of warfare across the spectrum. Therefore, to define hybrid warfare risks omitting key and unforeseen elements.

✓ Officials use the term “hybrid" to describe the increasing complexity of conflict that will require a highly adaptable and resilient response from U.S. forces without the need to articulate a new form of warfare.

✓ The term “hybrid" and hybrid-related concepts appear in the DOD overarching strategic planning documents (e.g., 2010 Quadrennial Defense Review Report); however, “hybrid warfare" has not been incorporated into DOD doctrine.

Traditional militaries find it difficult to respond to hybrid warfare. For example, if a collective defense pact such as NATO is uniformly uncertain of where an attack emanated how is a timely response possible? Conventional power is often insufficient to counter a hybrid threat. Often the conflict evolves under the radar and even a "rapid" response turns out to be too late. Overwhelming force is an insufficient deterrent. Many traditional militaries lack the flexibility to shift tactics, priorities, and objectives on such a dynamic basis due to their decision making and political authority granting mechanisms.

After in-depth discussion within the SERA 28 Committee-1 we agreed on the key characteristics of Hybrid warfare in order to provide a contextual framework in which to address our assignment:
Hybrid-warfare is not a new concept.

The use of asymmetric capabilities alongside conventional has been used by both state and non-state actors throughout history.

What has changed is the proliferation of dual-use technologies that act as a real force multiplier for both allies and adversaries alike.

These technologies know no boundaries and as such the theatre of operations now extends back from what was a front line in a foreign country right into our own sovereign states.

Because these technologies allow adversaries to threaten our own countries remotely or locally the distinction between defense and security has become blurred.

Research question and methodology

Hybrid Warfare – Unmanned Platforms and Combatant Enhancement – New Strategic Challenges for the EU?

Committee one accept that unmanned platforms and combatant enhancements do pose a new strategic challenge to the EU.

The scope of this paper is to examine the strategic implications that follow from the proliferation of unmanned platforms and combatant enhancements and their use by allied and enemy forces. We will examine a number of key technology areas and explain why each one represents a real strategic challenge in its own right:

- Unmanned Platforms;
- Combatant enhancements;
- Biological enhancements;
- Biometrics;
- Encryption;
- Social Media.

Once the strategic implication has been explained a series of recommendations will be provided for industry, policy-makers and society.

Unmanned platform

The strategic challenge posed by unmanned platforms is clear from their projected use in conflicts across all domains, from the smallest to the largest systems (see table 1) and at all levels from the tactical to strategic. For the purposes of this paper we will be examining UAVs in more detail than their land and maritime counterparts. Naval unmanned systems are in their relative infancy vis-à-vis air systems. The UK and France currently have a collaborative program examining the potential of such systems in a mine countermeasure role. Similarly in the land domain unmanned systems have been almost exclusively used in an Explosive Ordinance Disposal (EOD) role. The British Army recently accepted into service the Terrier Armoured Engineering Vehicle. This tracked system the size or a regular APC can be remotely operated...
to allow tasks to be completed in hostile environments where commanders if given the choice would not put personnel in harms way. Unmanned air systems on the other hand have been operational globally for well over a decade. Their use has proliferated and the barriers to entry for potential users steadily eroded. Their use by all actors, state and non statenon-state, has given rise to a number of ethical, legal and operational questions that remain to be fully addressed.

In current and future conflicts, military experts see UAV as frequent threats in all scenarios, e.g. terrorist attacks, hacking and hi-jacking, covert surveillance, smuggling, reconnaissance and correction of artillery fire. There are no barriers to entry for non-state actors to acquire UAVs for their activities. As such UAVs will be available and be in use by all forces.

Many of these cheap systems are simple enough to only require the most rudimentary of training. Will nation state air forces be reduced to a generation of gamers armed with a hand held controllers. The balance of power will be more difficult to calculate given that the UAV market is so heavily fragmented. Each actor will have differing amounts of UAVs with differing capabilities. The reality of the strategic challenge posed by these systems is highlighted by the proliferation of micro drones (those that weigh less than 2kgs). The micro drone could be easily equipped with a small warhead. Such a system could attack a static position or mobile unit from any direction and most worryingly is able to exploit a lack of top-based protection. This would render many existing self-protection and armour systems useless. In addition, UAVs can remove the advantage that well trained formal armies had over their less organised non-state actors by providing reconnaissance capabilities that allow poorly trained artillery units to correct their fire in short-time.

To counter these threats, the reconnaissance and combating of UAVs must be dramatically improved which will present a significant challenge. Small signatures, high speeds and the need for highly accurate three-dimensional surveillance must all be addressed. Currently this deficit results in very short reaction times for friendly forces. As such Europe’s military industrial complex must make a concerted effort to develop the specialized systems necessary to create a highly-responsive reconnaissance and command system.

**Considerations in the Passive Countering of UAVs**

Passive technology areas that could be prioritised in order to counter UAVs include:

- ✓ Sufficient means of protection against penetration from above (shrapnel, small bullets);
- ✓ Means to prevent the possibility that small UAVs can operate near a platform or in fact manoeuvre sufficiently close to the vehicle in order to enter it.

**Considerations in the Active Countering of UAVs**

The following capability requirements are highlighted as areas for European industry and procurement agencies to consider when contemplating threats against mobile land platforms:

- ✓ Ability for hard kill of UAVs considering possible collateral damage of the crash (see table 4);
✓ Ability for hard kill respectively taking the control over the UAV (see table 3);
✓ Ability for jamming of the sensors of UAV;
✓ Ability to undermine the ignition of the effectors.

Early Detection and Identification of Potential UAV Threats

It is necessary to be able to track any UAV. Countering the target with active protection means that industry must develop the capabilities to be able to discriminate, classify and identify targets on an ad-hoc basis in a timely fashion. The following capability requirements include:

✓ Ability to acquire agile targets in an urban terrain;
✓ Ability to acquire targets of all sizes;
✓ Ability to acquire very slow moving threats including targets in the hover.

Detection methods

Visible (possibilities)

✓ Eyes and via electro-optical devices;
✓ Infra-red.

Visible (challenges)

✓ Dependent on weather conditions;
✓ Short distance;
✓ Short reaction time;
✓ Several same type of UAVs;
✓ Hot enough hot for infra-red.
Electromagnetic (possibilities): radars or analysis of electro-magnetic spectrum
✓ Longer distance.
✓ Electromagnetic (challenges)
✓ Small radio signature.

Recommendations and Conclusion

UAVs are proliferating rapidly, they are cheap and easy to use and as such represent a strategic threat in being able to alter the military balance by undermining regular militaries’ traditional technological advantage. Industry has been slow to respond and nations slow to develop requirements or recognize the threat posed by such systems.

European governments and industry must begin to address the knowledge deficit by dedicating resources to develop tools, detectors, weapons and CONOPS to counter UAVs. In addition to this there are numerous legal and ethical issues that lawmakers will need to address. If lawmakers do not get ahead of the technology now they will forever be playing catch-up allowing criminals and hostile forces to act with impunity whilst friendly forces’ operations could become subject to legal challenge due to the existing ambiguity. Industry, politicians and the military must be aligned and working as one in order to confront this strategic challenge.

Combatant enhancements

War is an all-too-human affair, and it perhaps will always cost human lives. This is a terrible cost, but one which science and technology hopes to ease. History has seen an evolution of defensive and offensive technologies – from shields and body armour to more accurate and longer range artillery – that are aimed exactly at minimizing the human cost, at least on our own side. In today’s Digital Age, we are inventing entirely new and imaginative paradigms with military robots, cyber-weapons, and other technologies that promise to replace the organic, soft-bodied combatant and better protect noncombatants as well.

According to the Cambridge Dictionaries Online, the definition of enhancement is “to improve the quality, amount, or strength of something”, consequently, at a very basic level, all items soldiers carry and use could be considered enhancements to aid them in battle. Starting from this statement it is possible to define “Combatant Enhancements” as those technologies that augment the capabilities of warfighters at the individual level, used to modernize their equipment and ancillaries through the maximization of the synergy between the man and high-tech content, recognising the principle of modularity and adapting them to any type of operational and environmental scenario.

Recent operational experiences and technological improvements have increased equipment obsolescence rates and, consequently, the need to develop a soldier combat system that,
recognising the complexities of modern combat and capability procurement, must enhance the soldier’s performance, reduce the soldier’s burden and target the capabilities of the adversary. The emerging situations suggest that military forces will continue to play a decisive role in countering possible adversaries. Moreover, there has been a rapidly increasing proliferation of military technology and hardware with non-state actors having access to conventional military capabilities and other capabilities easy to find on the market like cyber-attack systems, unmanned aerial systems etc.. To grant effective success against adversaries that recently appeared in conflicts and incidents, it is necessary to provide forces with the right combination of capabilities.

It would be useful to take into consideration the basic functional characteristics and skills of the “soldier of the 2000s” or “Future Soldier” listed by NATO, as follows:

✓ Survivability: intended as the achievement of effective physical protection of the soldier, improved with the integration of emerging technologies against the full range of threats (ballistic protection, anti-NBC, anti-laser, fire and observation equipment), through the mitigation of weight and thermal effects, the reduction of signature across the electro-magnetic spectrum and reducing the probability of being seen and/or targeted;

✓ Lethality: its improvement does not only stem from the new technologies related to weapons and ammunition that provide better engagement options, but also from those relating to the equipment for target acquisition, fire control systems, communications and information management tools to achieve shared understanding and allow timely engagement (calibre, grenade launcher, day/night view modular pointing system);

✓ Command, Control, Communications, Computers and Information (C4I): integrate and develop communication systems and sensors to enhance both the global fighter’s situation perception and its capacity to act effectively (encrypted communications systems, data presenters, personal computer/handheld, night vision binocular, friend/foe identifier and targets designator);

✓ Mobility: further optimizing the ergonomics of materials, the weight of equipment, the optimization and modularity of loads; improving operations in a nightscape with enhanced situational awareness (lighter weapons and equipment, breaching tools, artificial mobility devices - e.g. exoskeletons - and enhanced human physical performance levels to increase range, speed and duration of operations);

✓ Sustainability, further optimizing the operating cycles of electronic equipment using innovative materials in the power generation and management systems sector and rechargeable batteries and providing combatants with supplies augmenting unmanned logistic systems including robotics and unmanned aerial systems.

To provide dismounted soldiers with the best equipment to face the modern battlefield, military and industry communities should work closely taking into account several factors such as costs, budgets, logistics, planning procedures and acquisition processes. Unfortunately, because of differences in requirements, scope and timing of the countries’ soldier modernisationmodernization plans, a collaborative programme between different nations seems unlikely. This results in replication, the wasting of resources and Europe remaining extremely uncompetitive.
The development roadmap for the current systems will include the following technologies/capabilities listed below. Europe still has sufficient time to begin to co-ordinate its efforts and resources for best strategic effect.

- Augmented reality combat goggles able to record everything a soldier sees and also to provide an information overlay (navigation instructions, intelligence on enemy sites) and real-time translations of local languages tools;
- Next-generation body armour using layered scales for light, flexible protection able to be fine-tuned to specific roles;
- Exoskeletons agile enough to fit underneath a soldier’s clothing to help soldiers carry extra weight without risking the joint and back injuries that typically accumulate in the field and boost their endurance;
- Hummingbird-size drone that can be carried in a pocket for fast deployment and fly about a mile, beaming back full-motion video and snapshots as it goes;
- Self-guided bullets using tiny sensors and fins to change direction mid-flight

New ethical challenges are arising from the technological developments in stem cells, genetics, neurosciences, robotics, and information technology. These developments have created ethical vacuums, situations in which our technology has outstripped our ethical framework. These ethical, legal and policy making challenges will be examined in more detail as a number of the potential future combatant enhancements are addressed in later sections of the paper.

**Recommendations**

Soldiers will continue to be the fundamental resource, the common denominator on current and future battlefield. The European defence industrial-base has to continue to focus on the development of new capabilities in order to strengthen soldiers’ survivability, lethality, C4I, movement and sustainment abilities. From a technical perspective the key areas of focus could include:

- Lighter weight and longer battery life of electronic devices available;
- Lower weight and greater effectiveness of ballistic protections;
- Technological development of sensors and devices that improve the protection and effectiveness of the fighter.

From a European policy perspective consideration should include:

- Europe making a concerted effort to remove the usual lag between technology’s adoption and the legislative catch-up that usually follows. Legislation must be future proof having contemplated as many future technologies as possible;
- Close collaboration between nations in developing required capabilities;
- Requirements defined by European nations in order to drive industries development phase;
- Cooperation between industries when requirements are defined;
- Centre of excellence for developing capabilities.
Biological Enhancements and Exoskeletons

Science fiction, or actual U.S. military project? Half a world away from the battlefield, a soldier controls his avatar-robot that does the actual fighting on the ground. Another one wears a sticky fabric that enables her to climb a wall like a gecko or spider would. Returning from a traumatic mission, a pilot takes a memory-erasing drug to help ward off post-traumatic stress disorder. Mimicking the physiology of dolphins and sled-dogs, a sailor is able to work his post all week without sleep and only a few meals.

All of these scenarios are real military projects currently in various stages of research. This is the frontline of the Human Enhancement Revolution — we now know enough about biology, neuroscience, computing, robotics, and materials to hack the human body, reshaping it in our own image. Technology can make up for mankind’s frailty. Unlike other animals, we’re not armed with fangs, claws, running speed, flight, venom, resilience, fur, or other helpful features to survive a savage world. We naked apes couldn’t survive at all, if it weren’t for our tool-making intellect and resourcefulness. And therein lies a fundamental problem with how Homo sapiens wage war: As impressive as our weapon systems may be, one of the weakest links in armed conflicts—as well as one of the most valuable assets—continues to be the warfighters themselves. Hunger, fatigue, and the need for sleep can quickly drain troop morale and cause a mission to fail. Fear and confusion in the “fog of war” can lead to costly mistakes, such as friendly-fire casualties. Emotions and adrenaline can drive otherwise-decent individuals to perform vicious acts, from verbal abuse of local civilians to torture and illegal executions, making an international incident from a routine patrol. And post-traumatic stress can take a devastating toll on families and add pressure on already-burdened health services.

To be sure, military training seeks to address these problems, but it can do only so much, and science and technology help to fill those gaps. In this case, what’s needed is an upgrade to the basic human condition. We want our warfighters to be made stronger, more aware, more durable, more maneuverable in different environments, and so on. The technologies that enable these abilities fall in the realm of human enhancement, and they include neuroscience, biotechnology, nanotechnology, robotics, artificial intelligence, and more.

Considerations

Established standards in biomedical ethics—such as the Nuremberg Code, the Declaration of Helsinki, and others—govern the research stage of enhancements, that is, experimentation on human subjects. But “military necessity” or the exigencies of war can justify actions that are otherwise impermissible, such as a requirement to obtain voluntary consent of a patient. Under what conditions, then, could a warfighter be commanded (or refuse) a risky or unproven enhancement, such as a vaccine against a new biological weapon? Because some enhancements could be risky or pose long-term health dangers, such as addiction to “go pills”, should military enhancements be reversible? What are the safety considerations related to more permanent enhancements, such as bionic parts or a neural implant?
Once ethical and safety issues are resolved, militaries will need to attend to the impact of human enhancements on their operations. For instance, how would integrating both enhanced and unenhanced warfighters into the same unit affect their cohesion? Would enhanced soldiers rush into riskier situations, when their normal counterparts would not? If so, one solution could be to confine enhancements to a small, elite force. (This could also solve the consent problem.) As both an investment in and potential benefit to the individual warfighters, is it reasonable to treat them differently from the unenhanced, such as on length of service and promotion requirements? On the other hand, preferential treatment to any particular group could lower overall troop morale.

From a legal and policy standpoint how do enhancements impact international humanitarian law, or the laws of war? The Geneva and Hague Conventions prohibit torture of enemy combatants, but enhanced soldiers could reasonably be exempt if underlying assumptions disappear—that humans respond to a certain level of pain and need sleep and food—as I suggested at the beginning. Further, enhancements that transform our biology could violate the Biological Weapons Convention, if enhanced humans (or animals) plausibly count as “biological agents“, which is not a well-defined term. International law aside, there may be policy questions: Should we allow scary enhancements, which was the point of fierce Viking helmets or samurai masks? Could that exacerbate hostilities by prompting charges of dishonor and cowardice, the same charges we’re now hearing about military robots?

Military-civilian issues certainly need to be considered. Most warfighters return to society as civilians and would carry back any permanent enhancements and addictions with them. The US has about 23 million veterans—or one out of every 10 adults—in addition to 3 million active and reserve personnel, so this is a significant segment of the population. Would these enhancements, such as a drug or an operation that subdues emotions, create problems for the veteran to assimilate to civilian life? Would they create problems for other civilians who may be at a competitive disadvantage to the enhanced veteran who, for instance, has bionic limbs and enhanced cognition?

**Exoskeletons**

The EU faces a strategic challenge by the growing use of exoskeletons in the military. In order for the EU’s military forces to enjoy a military advantage and to compete with the US in this field its industries will need to overcome a series of technical hurdles. This will require patience and a large amount of funding given the scale and history of US attempts to date. Even as these technical challenges are overcome there are many ethical, legal and social issues that now need to be managed at a supranational level. Many of these issues have already started to be discussed due to the ongoing application of these technologies for civilians with restricted mobility.
Considerations

The ability to augment otherwise healthy individuals with military-grade exoskeletons starts us down the slippery slope of human enhancement, a challenging area with broad repercussions in conventional society ranging in applications from medicine to sports. Additionally, in transforming soldiers into quasi-machines, we risk further dehumanizing warfare and its human actors, raising the potential for abuse not only by the enemy, but by commanding officers. To join a military has always been to accept one’s role in a larger cause, and with certain diminished freedoms as a result – but the intrinsic value of a warfighter has never before been routinely confused with the merely instrumental value of a tank or a missile or a rifle. However, at some point a change in degree begins to be seen as a change in kind. If the physical abilities of warfighters become too great, it may take great restraint on the part of their commanders and even their peers to see them, not as a killing machine, but as a person – even if they are enhanced. This capacity for exploitation can also affect civilian workers who will use exoskeletons in heavy industries. Even corrective uses associated with restoring abilities to the disabled raise social justice concerns relating to the availability of, and accessibility to, this life-altering technology. Therapeutic implementations may also compel us to redefine nontrivial concepts of disability and ableness in light of the growing capacity to technologically supplement human frailties; additionally, current legal and regulatory structures may be unable to appropriately fit newly abled individuals within current disability conventions. From a military stand-point how would society view having what were previously considered disabled soldiers on the front-line? How in practice could this dual-use technology be properly controlled? If stringent controls were put in place this could prevent disabled civilians from benefiting from these technological advances. On the other hand, such technologies in the hands of criminals or terrorists would pose a significant force multiplier and threat to friendly forces.

Not only will exoskeletons likely raise novel legal issues relating to product liability, but the potential to implant brain machine interfaces (BMIs) within the posterior parietal cortex, resulting in preconscious control over the exoskeleton, may challenge longstanding near-universal tenets of criminal law. In most jurisdictions, an individual cannot be guilty of a crime if they lack the threshold mens rea and actus reus (i.e., a guilty mind resulting in a guilty action). BMIs, particularly those supplemented with artificial intelligence, could result in arguably involuntary actions that confound criminal culpability and conceivably put into question even more fundamental issues of free will.

Recommendation

In anticipating, promptly acknowledging, and perhaps even tackling these and other concerns, we can preempt and preclude potentially hampering legislation and regulation that might inhibit innovation. The EU needs to create a mechanism to manage this evolution to guarantee that this technology enhances our economic well-being and security rather than undermining it.
Biometrics

One of the biggest challenges facing the European Union with regards to countering terrorism is to discriminate/identify between law abiding citizens and those that wish to do us harm. Hybrid warfare sees the battlefield become all pervasive where physical borders are no longer respected. In Europe many attacks have been perpetrated by home-grown terrorists, European nationals radicalized over the internet. As such regardless of whether the perpetrator is a foreign national or EU citizen they generally require the support of others. Many guerilla wars and terrorist campaigns have highlighted the fact that those carrying out such acts must enjoy the support of a community because without it, it is harder to remain undetected from the authorities. Authorities struggle to know whether people of interest are currently here in Europe, in the Middle East or elsewhere. As such there is a growing willingness amongst the citizens of many countries within the EU and particularly those subject to terror attacks in recent times to allow a more invasive security structure in order to help foil future attacks. One such security mechanism is biometrics.

Biometrics poses a strategic challenge to the EU because in reality there are no perfect technical biometric systems. Systems suffer from many shortfalls including distance of detection and high false alarm rates. The tendency towards “complete” security means in the long run a tendency towards decreasing social trust, creating secret systems and a society based on secrecy instead of trust and transparency. From this perspective, biometric systems are paradoxical: they increase the digital transparency of people while at the same time promoting manipulation, disguising, concealment, blurring, and bluffing. Dealing with this paradox is a major issue for information ethics. The illusion of a completely transparent and open society is no less dangerous than that of a society based on secrecy and security, over-protecting itself against potential spoofing attacks.

The human body offers much more data than is required for authentication/identification purposes. For instance, some systems installed at airports include a body/face temperature check. So far, this has mainly been used to control or prevent SARS epidemics. The possibility of excessive collection of physiological data is linked to the possibility of unfair discrimination against members of the public. For example, if such technologies were used in commercial realms of if and an insurance company began checking its potential customers’ healthusing information obtained by an integrated biometric system, persons seeking its services could be discriminated against.

As camera surveillance is becoming commonplace in societies around the world, the possible unregulated increase of biometric authentication/identification nodes within an individual’s daily life could also provoke extreme marketing by commercial enterprises. This is particularly the case as biometrics measurements are not only physical but also behavioral. Although this evokes science-fiction scenarios such as Minority Report, it is true to say that societies are indeed creating the frameworks for such a surveillance environment and, considering all the benefits of biometrics- when used appropriately - its use is likely to increase.
Recommendations

Although it is important to note that most privacy advocates seem to focus on the potential abuse of biometric technologies rather than their benefits, the establishment of legal/ethical frameworks and standards for the safe storage and protection of an individual’s biometric data is imperative. In order to achieve this, legislation must be updated.

The EU could look to make Biometric the most sensitive of information types since data derived from individuals’ unique — and irreplaceable — physiological characteristics is nothing but personal. This argument can be further supported from a slightly more technical perspective. In database management terms, if the (biometrically derived) raw data uniquely identifies an individual then it has the potential of a primary key (unique identifier). Under any other circumstance, a record could have a new primary key assigned (for example, even a tax file number can be replaced), whereas the biometric unique identifier as a primary key is irreplaceable. Thus, one can’t affix a new iris, fingerprint, etc. Furthermore, biometric data obviously acts as the primary key that can reveal other sensitive information. In fact, this is a good reason biometric data should not only be deemed as sensitive information but as the ultimate personal information. No other sensitive data has this ability to uncover all other personal details about the particular individual. In fact, biometric data can be used to accumulate all additional information since it has the potential to become the ultimate tracking technology — given more widely spread scanning nodes (surveillance cameras, biometric ATMs, airports, etc.). In contrast, one’s personal political opinions, sexual preferences or philosophical beliefs are not mutually revealing.

Taking these concerns into account the EU needs to strategically invest in harnessing the power of biometrics for the protection of its societies by supporting industry in exploiting its many applications including integration of biometric sensors on unmanned platform and in equipment for the enhancement of the individual soldier. It is not easily apparent that companies are or plan to invest in this area without government direction.

Regardless all of these activities must be carried out within an international context where the core technologies and biometric data generated is shared. Like all intelligence it is generated in order to be shared and traded in order to gain access to a larger body of intelligence held by allied organisations and nations. This will call for additional guarantees around data protection when handing over biometrics of European citizens to foreign entities. It will also call for an open debate between governments and their citizens in order to build trust and communicate the upside vis-à-vis the risks connected with the collection and sharing of such data.
Encryption

Information security has always been an essential element of military communications. In the modern world civilian and military means of communication have continued to converge. Law enforcement agencies had enjoyed until recent times the means to intercept communications and with relative ease exploit its content. This situation has dramatically altered with the advent of commercial enterprises providing highly encrypted means of communication more often than not on a free basis. Encryption is a significant “combatant enhancement” allowing individuals the unhindered clandestine capacity to organise themselves, recruit to their organisations, facilitate networking, execute operations and share best practice and knowledge. This is all the more serious as the increasing use of encryption makes lawful interception by the relevant national authorities technically difficult or even impossible. Signals intelligence has traditionally been the primary source of actionable intelligence for law enforcement agencies. However, this source will continue to be eroded away if encryption continues to proliferate unchecked or government agencies do not keep pace with ever evolving communication technologies.

Western governments and supra-national organisations are a long way from presenting a unified front in agreeing how they intend to address the encryption issue. Instead each nation or organisation is aggressively lobbying for their pro or anti-encryption position. These positions have become better known as governments have commented on the issue in the wake of the terror attacks in France and Belgium. Even within EU bodies, diametrically opposed policies are being proposed. For example, the EU’s Counter-Terrorism Coordinator has advised that internet and telecommunications companies should be obliged to share encryption keys with government agencies to help them fight terrorism. These views contrast with the European Commission’s Vice President who has stated that “in the European Commission we never had, and we won’t have, any kinds of plans to create back doors. We don’t want to destroy people’s trust by creating back doors and that if there were back doors then sooner or later somebody would misuse them”. Even ENISA the European cybersecurity agency has argued against backdoor measures not least because encryption is essential in protecting citizen’s data against criminals. Law-abiding citizens would be the ones to lose out on a law that bans or weakens encryption. This view is representative of a wider concern that any weakening of encryption to support law enforcement should not undermine the EU’s tough data protection rules that enshrine privacy on par with other rights like freedom of expression.

As such being pro or anti-encryption reads across to being either pro privacy versus pro national security. French politicians are debating proposals that may hand tech company executives with prison sentences of up to five years as well as fines of around $390,000 if they refuse to provide encrypted information to government agencies. Similarly, the United Kingdom’s Prime Minister has floated the idea that encrypted online messaging services such as WhatsApp and Apple’s iMessage should be banned whilst Hungary has proposed banning encryption software altogether. Meanwhile Germany and the Netherlands remain opposed to such policies. The Dutch government has stated that weakening encryption would make encrypted files vulnerable to criminals, terrorists and foreign intelligence services. Ironically this also comes at a time when
the security community has been asking users to ensure they use the latest encryption and extend their passwords precisely because the arms race between encryption and the ability of computing power to break it is continuous.

Industry shares these concerns with Apple stating that a “key left under the doormat would not just be there for the good guys…. The bad guys would find it too”. This struggle has played out in the media where Apple has battled against the FBI’s demand for them to decode encrypted data on an iPhone that belonged to a suspect in the terrorist shootings that took place in San Bernadino, California.

A domino effect is predicted where if one country demands back-door access and it is provided other countries will quite rightly make similar demands. Industry would then be in a difficult position if law enforcement officials from an “unfriendly” country made requests for politically motivated surveillance. It was this dilemma that resulted in the introduction of end-to-end encryption in the first place removing industry from the equation where the encryption keys are in the hands of the sender and receiver of the communication.

**Recommendations**

With this in mind, in order for the EU to build consensus on encryption they will need to construct a solution that addresses the concerns of law enforcement whilst ensuring that the critical role that encryption plays for the EU’s citizens and the economy are not undermined.

Encryption is here to stay and a technology that government can no longer control. Unlike weapons of mass destruction there is no large infrastructure required to produce and distribute encryption. The technology is widely and freely available. Even if it was banned criminals would continue to use it whilst law abiding citizens made all the more vulnerable. The internet was never designed to be secure and layering encryption over it is the only way to ensure the confidentiality, integrity and authenticity of citizens’ interactions. As such anti-encryption legislation and backdoors are a futile response which the EU should avoid. Instead the priority is to identify the tools and resources that law enforcement/military officials need in order to fulfil their duties in a world where encryption is all pervasive.

Information sharing among European agencies must be improved. It is clear that the sharing of data is far from optimised and in investigations of both the Paris and Brussels attacks that the problem was not encrypted data but data that existed that was simply unavailable to the right authorities.

Creating a common and accessible pool of technical capabilities across the EU is essential. Many agencies are unable to access encrypted communications, hack individual devices giving direct access to a suspect’s computer or mobile phone or break encryption using “brute force”. A small number of countries have access to such tools but often the technology is limited and oversight and legal frameworks inadequate for their operation. EU countries should consider what capabilities are and will be required and develop a platform to consolidate and exchange them.
Greater co-operation between the EU and US will be required in order for EU agencies to gain access to US companies involved in telecommunications. In order for global agreements to be struck a European consensus on such measures is required.

The EU could also look to re-establish trust with its citizens who continue to harbour concerns over mass surveillance by providing evidence that quantifies the real problems law enforcement agencies are facing through the proliferation of encryption. Ultimately a lack of a common policy undermines the EU’s common digital market and obstructs its fight against terrorism and organised crime and as such must be addressed.

**Social media**

Social Media and related “Smartphone apps (hereafter just “Social Media”)” is strategically important to the EU for several reasons within the domain of “Hybrid Warfare”. “Social Media” has proven to be a very effective “Command & Control” platform in many recent conflicts, ranging from peaceful purposes in disaster relief (ex. 2010 Haiti, 2011 Christchurch Earthquakes) to a communication platform for insurgents in asymmetric conflicts like Afghanistan, Syria – ending in larger scale “Hybrid Warfare” scenarios like seen in Ukraine. The communication platform for “Social Media” is Global, relatively affordable and platforms/devices likes smartphones and tablets are readily available. The communication platform is not robust in full scale symmetric environments, but within the boundaries of “Hybrid Warfare” this is seldom an issue.

On top of the obvious advantages of availability, “Social Media” has also proven to be a very agile lightweight “Command & Control” tool, which gives the user a tool to facilitate fast decision-making – being able to: Observe, Orient, Decide and Act (ref. The OODA loop in Mil decision making). This agile way of conducting military operations, terrorist attacks etc. has often proven to be a huge challenge for conventional European military units – hence the need for the EU to take its countermeasures.

Just until recently, “Social Media” have been using communication technologies without encryption – enabling governmental intelligence services to tap into the information stream within local legal boundaries. “Social Media” providers have recently implemented very restrictive encryption technologies in their communication platforms, making it virtually impossible for governments to monitor – thus providing insurgents with the ideal “Command & Control” platform: Low cost, Global, Agile & Secure.

For the reasons above, “Social Media“ is a challenge but then again also an opportunity. We need to convert the current challenges to opportunities i.e. “combatant Enhancements“. In this transformation, we need to understand how we can transform information on “Social Media” into Intelligence. In this process, we will deal with some simple models on intelligence, selected for the purpose of mapping this to “Social Media“:
With the appearance of “Social Media”, we have seen this as being used for several purposes in the ladder of conflict within "Hybrid Warfare":

✓ Information sharing;
✓ Propaganda;
✓ Recruitment;
✓ Deployment;
✓ Armament enabling (Weapons, Procedures & Training);
✓ Situational awareness during operations.

“Social Media” gives the platform to the opponent to share intelligence. The availability makes this tool the preferred choice. On the other hand, EU defence and security forces will be enhanced, by having intelligence from “Social Media”, to intervene in conflicts at early stages of the conflict ladder:

✓ Create counter intelligence;
✓ Influence communities of interest;
✓ Anomaly detection, new patterns of action;
✓ Proactively preventing crimes/conflicts.

“Social Media” was originally a very easy, yet open way to share information. With the appearance of “Social Media”, we saw groups of people suddenly openly sharing information we would otherwise regard as relative private/secret. The only protection on this media in the beginning would be methods you would likewise use when talking on open telephony lines eg. Speaking in code.

The recent changes in technologies applied by global providers of “Social Media”, such as encryption, makes it impossible to monitor “Social Media” – thus moving “Social Media” out of the OSint domain.
**Recommendations**

- Improve our abilities in leveraging our OSINT capabilities on “Social Media” in general;
- Many countries in the EU have limited tools to make OSINT studies on “Social Media”;
- Make sure intelligence services can monitor encrypted communication technologies;
- Regulating the market for “Social Media”, to enable legal surveillance;

Make intelligence readily available for the combatants: Removing bureaucratic procedures, allowing fast and reliable information systems, make sure information is reaching the individual warfighter.

**Conclusion**

Hybrid warfare is nothing new. It will continue to encompass the full range of threats. What is new is the pace of change. It is extremely clear having researched this paper that the pace of technological change is leaving law makers, policy makers, military planners and tacticians as well as industry squarely in its wake. Technology is evolving so quickly that our national and international institutions and their internal processes are unable to keep pace. By the time new legislation has been approved the technology in question can in some instances already be obsolete. Unless a long term strategic view is applied our leaders will always be playing catch-up.

Without a strategic view, without pre-emptive policy and legislation a vacuum is created. Industry is unable to invest with shareholders uneasy at self-funding technologies that no government may ultimately buy. Even if technologies are developed, procured and enter service, governments may face legal action from members of their own armed forces or from enemy combatants or civilians affected by these new technologies that are being used without any legal framework in place. Society could well lose trust in its leaders if these technologies are abused or misused knowingly or accidentally.

The EU must take proactive measures to ensure that this vacuum is not created and that these technologies are recognized as providing Europe with a real edge, an advantage. This will be an economic advantage if industry is to lead the technologies introduction and widening of its scope of applications. For the warfighter the EU’s nations’ armed forces could enjoy a substantial edge over their adversaries and with the full faith and trust of its citizens.

The EU must enlist the support of technologists, industrialists, ethicists, economists et al that understand the trajectory of these technologies, how they will evolve and what considerations law makers must be conscious of. In essence the age old mantra of increased co-operation and collaboration will continue. This will also be necessary to ensure that the control of these technologies is managed correctly and that both the military and civilian communities can enjoy the life changing benefits that the technologies are capable of without any stakeholder group losing out.
Bibliography

Hybrid warfare definition
- The View from Oregon; Grand strategy and geopolitics from the perspective of the Pacific Northwest; Hybrid Warfare; 7 October 2014
- NATO Review / Deterring hybrid warfare: a chance for NATO and the EU to work together?; 2015
- NATO Review / Hybrid war – does it even exist?; 2015
- New Threats, New EU and NATO Responses, Clingedaal report; July 2015
- Hybrid Warfare; US Government Accountability Office; Ref: GAO-10-1036R; Released Sept. 13, 2010

Unmanned platforms
- Study results from German Federal Office of Bundeswehr Equipment, Information Technology and In-Service Support, BAAINBw K1.2

Combatant enhancements
- Building on Beersheba - Future Capability Discussion Paper One: The Soldier Combat System - Strategic Plans Branch, Army Headquarters 2014;
- Future Soldier - Systems Conference (FSSC) (20 – 21 October 2016, Prague, Czech Republic) leaflet;

Biological enhancements & exoskeletons
• http://science.sciencemag.org/cgi/content/full/350/6265/1176-a
• http://science.sciencemag.org/cgi/content/full/350/6258/270

**Biometrics**
- http://www.webopedia.com/TERM/B/biometrics.html;
- http://www.biometricsociety.org/about/definition-of-biometrics/;
- http://www.biometricnewsporal.com/biometrics_definition.asp;
- http://www.biometrics.gov/;
- http://www.capurro.de/biometrics.html;

**Social media**
- Why ISIS is winning the Social Media War (www.wired.com)
- The Challenges of Hybrid Warfare, Eva Hunter and Peret Pernik (ISSN 2228 2075)
- Social Media and Information Operations in the 21st Century, Nicholas Shallcross, Airforce Institute of Technology
Main references

The following tables list UAVs as per their classification followed by the means to detect, neutralise and kill such systems.

Table 1. NATO UAS Classification Guide

<table>
<thead>
<tr>
<th>Class</th>
<th>Category</th>
<th>Employment</th>
<th>Normal Altitude</th>
<th>Mission radius</th>
<th>Supported commander</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>Class I (less than 150 kg)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SMALL &gt; 20 kg</td>
<td>Tactical</td>
<td>(launch system)</td>
<td>Up to 5 000 ft</td>
<td>50 km</td>
<td>Tactical Unit</td>
<td>Hermes 90 Schiebel S-100</td>
</tr>
<tr>
<td>MINI 2-20 kg</td>
<td>Tactical</td>
<td>(manual launch)</td>
<td>Up to 3 000 ft</td>
<td>25 km</td>
<td>Tactical Subunit</td>
<td>AV-RQ-20 Puma, Elbit Skylark</td>
</tr>
<tr>
<td>MICRO &lt;2kg</td>
<td>Tactical</td>
<td>(manual launch)</td>
<td>Up to 200 ft</td>
<td>5 km</td>
<td>Platoon,</td>
<td>PRS-PD-100 DJI-Phantom</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Section, Ind.</td>
<td></td>
</tr>
<tr>
<td>Class II (150-600 kg)</td>
<td>TACTICAL</td>
<td>Tactical</td>
<td>Up to 10 000 ft</td>
<td>200 km</td>
<td>Tactical</td>
<td>Hermes 450 SAGEM Sperwer</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Formation</td>
<td></td>
</tr>
<tr>
<td>Class III (more than 600 kg)</td>
<td>STRIKE</td>
<td>Strategic/national</td>
<td>Up to 65 000 ft</td>
<td>Unlimited</td>
<td>Theater COM</td>
<td>RQ-170 Sentinel</td>
</tr>
<tr>
<td></td>
<td>HALE</td>
<td>Strategic/national</td>
<td>Up to 65 000 ft</td>
<td>Unlimited</td>
<td>Theater COM</td>
<td>RQ-4 Global Hawk</td>
</tr>
<tr>
<td></td>
<td>MALE</td>
<td>Operational/theater</td>
<td>Up to 45 000 ft</td>
<td>Unlimited</td>
<td>JTF COM</td>
<td>MQ-1 Predator Hermes 900</td>
</tr>
</tbody>
</table>

JAPCC Strategic Concept of Employment for UAS in NATO, 2010

Table 2. Detection methods

<table>
<thead>
<tr>
<th>Class</th>
<th>Visual</th>
<th>Acoustic</th>
<th>Radars</th>
<th>Spectrum analysis</th>
<th>Thermo camera</th>
</tr>
</thead>
<tbody>
<tr>
<td>Class I (less than 150 kg)</td>
<td>MICRO &lt;2kg</td>
<td>Problem</td>
<td>Problem</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>MINI 2-20 kg</td>
<td>Problem</td>
<td>Problem</td>
<td>Yes</td>
<td>Problem</td>
</tr>
<tr>
<td></td>
<td>SMALL &gt; 20 kg</td>
<td>Problem</td>
<td>Problem</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Class II (150-600 kg)</td>
<td></td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Problem</td>
</tr>
<tr>
<td>Class III (more than 600 kg)</td>
<td></td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

Baltic Institute of Advanced Technology, 2016
Table 3. Ways of neutralizing

<table>
<thead>
<tr>
<th>Class</th>
<th>Kinetic (artillery, missiles)</th>
<th>radio communications disruption</th>
<th>GPS disruption</th>
<th>Energy weapons</th>
<th>Fighter planes, new counter-UAV flying system</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Class I</strong> (less than 150 kg)</td>
<td>MICRO &lt;2kg</td>
<td>Problem</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>MINI 2-20 kg</td>
<td>Problem</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>SMALL&gt; 20 kg</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td><strong>Class II</strong> (150-600 kg)</td>
<td>Yes</td>
<td>Problem</td>
<td>Problem</td>
<td>Problem</td>
<td>Yes</td>
</tr>
<tr>
<td><strong>Class III</strong> (more than 600 kg)</td>
<td>Yes</td>
<td>No</td>
<td>Problem</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Baltic Institute of Advanced Technology, A. Ploksto, 2016

Table 4. Probability to kill

<table>
<thead>
<tr>
<th>Weapon Type</th>
<th>MICRO &lt;2kg 70 m</th>
<th>MINI 2-20 kg 1 000 m</th>
<th>SMALL &gt;20 kg 1 500 m</th>
<th>TACTICAL 150-600 kg 3 000 m</th>
<th>STRIKE &gt;600 kg 20 000 m</th>
<th>HALE &gt;600 kg 14 000 m</th>
<th>MALE &gt;600 kg 14 000 m</th>
</tr>
</thead>
<tbody>
<tr>
<td>Net-launching anti-drone systems¹</td>
<td>High</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Small Arms (5,56 – 12,7 mm)</td>
<td>Low</td>
<td>Low</td>
<td>Very low</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Artillery (20 – 40 mm)</td>
<td>Very low</td>
<td>Low</td>
<td>Low</td>
<td>Average</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>New artillery, new ammunition² (35 – 90 mm)</td>
<td>Very low</td>
<td>High</td>
<td>High</td>
<td>High</td>
<td>0</td>
<td>0</td>
<td>Low</td>
</tr>
<tr>
<td>VSHORAD missiles</td>
<td>0</td>
<td>0</td>
<td>Average</td>
<td>High</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>SHORAD missiles</td>
<td>0</td>
<td>Average</td>
<td>High</td>
<td>High</td>
<td>0</td>
<td>0</td>
<td>High</td>
</tr>
<tr>
<td>New counter-UAV flying system³</td>
<td>0</td>
<td>High</td>
<td>High</td>
<td>High</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Fighter air-air missiles</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>High</td>
<td>High</td>
<td>High</td>
<td>High</td>
</tr>
<tr>
<td>Lasers</td>
<td>High</td>
<td>High</td>
<td>High</td>
<td>Low</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>High-energy EM pulse</td>
<td>High</td>
<td>High</td>
<td>High</td>
<td>Average</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Radio disruption</td>
<td>High</td>
<td>Average</td>
<td>Average</td>
<td>Average</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>GPS Spoofing, jam</td>
<td>Average</td>
<td>Average</td>
<td>Average</td>
<td>Average</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Special forces against operators</td>
<td>High</td>
<td>Average</td>
<td>Average</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Indirect artillery fire against operators</td>
<td>Average</td>
<td>Average</td>
<td>Low</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

1 Runs on compressed gas or blank cartridge from the ground
2 Specialized air burst ammunition, with tungsten net, metal dust, plastic tape or small pellets, not invented yet
3 High-speed, fast maneuvering UAV with effectors like net launching system or specialized air-to-air missiles, not invented yet
Committee 2

Deception, Information and Cyber Warfare: how could Europe approach hybrid warfare levers to her advantage?

Pilots: Viggo LEMCHE, Jolanta SWIESCIAK

Members of the Committee
Barbara STOKLASOVA (Chair)
Scott ROBERTSON (Secretary)
Kari THURNHOFER
Marcus SHULZE
Trine OEKSNEBJERG
Frederic MOURET
Fabrizio D’AMBROGIO
Terje NYLAND (Royal Norwegian Navy)
Robert LIMMERGARD
Santiago TELLADO MATAMOROS
Bruno LANG
“For to win one hundred victories in one hundred battles is not the acme of skill. To subdue the enemy without fighting is the acme of skill.”

Sun Tzu, Chapter 3, Offensive Strategy, The Art of War.

The main papers within the EU dealing with security are the European Security Strategy 2003 (ESS) [1] and the implementation of this strategy 2008 [2]. Neither paper deals with the concept of “Hybrid warfare” thus require an urgent refresh and regular updating. The term “Hybrid” means that different “warfare”-methods are used at the same time or “blended” together to meet an actor’s desired outcomes. The ESS describes specific points such as information-warfare, cyberwarfare and energy security but not in combination. “Hybrid warfare” can also be a combination of regular and irregular methods, deception and economic warfare or at least sanctions as those between China and Japan [3] but also most recently between the EU and Russia over tensions in the Crimea and Ukraine [4] and [5].

In order to address the complexities of hybrid warfare Committee 2 developed a risk based analysis approach supported by the development and use of a high level dynamic model. This approach enabled the assessment of both the benefits and disbenefits of the potential for the EU to both deploy and bear the brunt of hybrid warfare. It also provides decision makers and analysts a tool set with which to model actions and outcomes before making any commitments to one or more courses of action.

The paper then lays out these vulnerabilities and those levers that the EU could avail itself of. In summary, although it is a direct threat to the EU and its member states, hybrid warfare may allow the EU to commit to courses of action intended to deliver EU strategic objectives whilst remaining within the spirit of the EU, International treaties and accepted “norms of behaviour”, without resorting to traditional military actions or inhibiting other partner’s freedom of action. To quote Sun
**Aim of this paper**

Committee 2 were tasked to “draft a “food for thought” paper discussing the perspectives for Hybrid Warfare in the area of Deception, Information and Cyber warfare. How could Europe approach hybrid warfare levers to her advantage?”

**Background**

**The Westphalian System**

National and International thinking about sovereignty, “the State’, “the People’, “Nation’ and how States and later “Nation States’ were expected to behave and interact were shaped by the outcome of the Thirty years war and the “Peace of Westphalia’ signed in 1648 by the major Continental European powers involved in the war including the Holy Roman Empire, Spain, France, Sweden and the Dutch Republic. This treaty [6] set out three main principles which explain the Peace’s significance and its on-going effect on the world today:

✓ Sovereignty of states and the fundamental right of political self-determination;
✓ Legal equality between states;
✓ Non-intervention of one state in the internal affairs of another state.

The so called "Westphalian System" has endured and been incorporated in International Law and Treaties, e.g., the UN Charter [7].

**Challenging the Westphalian System**

However, the very concept of Westphalian sovereignty and its applicability in practice as the "international norms" in the evolving 21st Century have been questioned due to:

✓ The rise of internationalism e.g., international intervention within "failed states";
✓ Globalisation e.g., the rise of multinational corporations, and;
✓ Interdependence, e.g., the links between the various global stock markets and international trade in oil and other natural resources.

The fall of the former Soviet Union, the continued evolution of the European Union (EU), expansion of NATO and NATO involvement in Afghanistan and other “Out of Area Operations”, a resurgent Russia and the continual growth of low cost Information Technology, smartphones and the all-pervasive and ubiquitous “internet” and “cyberspace" mean that the concepts of national integrity and sovereignty have less clarity than in previous centuries.
Russia and Hybrid Warfare

The annexation of Crimea and the offensive against Ukraine by Russia was the first time since the end of World War II that a European State took over parts of another European State by force. This alone presents a challenge to European decision making, political consensus and the European Security and Defence Policy. Beyond that however, the Ukraine crisis revealed another challenge that Europe is facing which culminates in the question “How to deal with hybrid threats?”

President Putin’s hybrid warfare strategy against Ukraine relies on the combination of conventional military and – to an even larger scale – on unconventional means. It was planned and executed with the clear intention to stay below level of armed aggression in order to avoid activation of collective defence commitments on the basis of existing treaties such as NATO Article 5 [8] and the EU’s Article 4.2 [9], see Annex A: Treaty Text Excerpts.

In other words: to reach the goals traditional gained by waging a “successful” conventional war but without becoming attracting too much International outrage and condemnation but also not inhibiting allies and partner’s freedom of action. In this sense hybrid warfare can be understood as something of a game changer: turning the existing ideas and strategies of countering threats imposed on Europe’s security upside down.

Hybrid warfare is often characterised as the comprehensive approach of the European Union “but gone over to the dark side of the Force”[10]. Additionally, the idea of combining a set of measures (covert action, deception, arms delivery etc.) has always been key part of warfare and security politics on either side throughout both the cold war and the post-cold war eras. However, dismissing hybrid warfare as an “old story” is definitely misleading; a closer look reveals a different and probably even more alarming picture: the extensive use of deception and information as central elements of a hybrid warfare strategy – as it became evident during both the Crimean and Ukraine crisis – led to a fundamental change and revaluation of warfare methods. The role of unconventional means became increasingly important for political and strategic goals and have, as former Chief of Staff of General Gerasimov puts it [11]:

“\textit{In terms of the scale of the casualties and destruction – the catastrophic social, economic, and political consequences – such new-type conflicts are comparable with the consequences of any real war. The very "rules of war" have changed. The role of non-military means of achieving political and strategic goals has grown, and, in many cases, they have exceeded the power of force of weapons in their effectiveness.}”

In this respect Crimean and Ukraine Crises were not “business as usual”. However, experts are clear that actions and tactics imposed on “New Russia” cannot serve as the sole model or blueprint of hybrid warfare tactics or hybrid threats. Future hybrid threats are difficult to anticipate and will most likely be of a completely different design or “blend” or “recipe” and character. As a consequence, the idea of pre-emptive measures on the basis of already existing
or new contingency plans to counter hybrid threats beforehand misses the point. Instead we need to develop a series of challenging questions to establish a hybrid strategy on an EU level:

✓ To get a transparent picture on own vulnerabilities in order to be able to define the “attack surface” on a continuing basis;
✓ in order to derive realistic scenarios that can be used to inform our analysis, and;
✓ To organise related (counter) measures suitable to address existing/emerging risks.

The deployment and continued development and refining of “hybrid warfare” provides its users with another comprehensive approach to meeting their goals whilst avoiding or at least minimising the potential adverse political, military and socio-economic effects of symmetric and asymmetric war and depending on the user challenging the “international norms”.

Introduction

What is "Hybrid warfare?"

The term “hybrid warfare” means different things to different people depending on contextual settings. Therefore, Committee 2 decided that we were not going to attempt to offer a definition of “hybrid warfare” but instead identify some of the key components and concepts that comprise “hybrid warfare”.

Hybrid Warfare: High level Concepts and Components

✓ “Hybrid warfare is not new”. In their translated paper 1999 [12] Senior Colonels Qia Liang and Wang Xiangsui detail a military strategy based on confrontation by means other than traditional military power and technology. In his 2002 paper [13] Nemeth lays out an analysis of a hybrid war using the Chechen war as a case study. This paper draws on earlier works from the late “90’s;
✓ Russia did not invent “hybrid warfare’, it has simply proven adept at “blending’ the components of hybrid warfare to achieve its strategic goals [11];
✓ Hoffman’s seminal paper in 2007 [14] states:

“Hybrid Wars can be conducted by both States and variety of non-state actors. Hybrid Wars incorporate a range of different modes of warfare, including conventional capabilities, irregular tactics and formations, terrorist acts including indiscriminate violence and coercion, and criminal activities. These multi-modal activities ... are generally operationally and tactically directed and coordinated within the main battlespace to achieve synergistic effects.”

✓ The major components of a “hybrid warfare strategy include:
  • “Lawfare’ [12]: the use of proxy transnational or non-governmental organisations to effect a favourable policy change;
• Economic Warfare [12]: taking advantage of globalisation and Interdependence to inflict harm on the economies of other nations without resorting to traditional offensive military action, whilst noting the potential for unforeseen impacts on your own economy as a result;

• Network warfare [11, 12]: attacking “computer networks” to destroy, disrupt or interrupt key IT nodes that your adversary depends on which may range from air defence networks, Command and Control nodes to electricity and water supplies and “softer” uses such as “smearing” a political opponent;

• Terrorism [12, 14]: to gain some advantage, or to cause substantial loss of life or infrastructure damage as a means of bringing pressure against the targeted nation, society or grouping;

• Omni-directionality [14]: such that commanders and political leaders have a wider “worldview” encompassing political environment, economics, culture, religion and moral factors as well as the traditional military battlespace comprising the air, land, maritime, space and cyberspace environments;

• Synchrony [14]: the ability for the political and military commanders to take omni-directionality and deliver synchronised effects in the real world in the same period of time;

• Asymmetry [13, 14]: this term has multiple meanings but here it is intended to mean that the actors have very different views regarding the usability of hybrid warfare components as well as recognising the potential disparity between the actors when considering “power” and resources to bring to bear to the issues;

• Deception and misinformation are key components within “Hybrid Warfare” and are ably described by Sun Tzu [15]:

**Hybrid Warfare and the EU as a political Entity**

On a general level Europe has vulnerabilities in four different areas:

**Territorial Integrity**

Since the end of the Cold War the European States have been reducing their military power constantly. This period of disarmament over the last 25 years has led to significant reduction of materiel and human resources and - quite frankly - to a shortfall of military forces across all EU Member States. Despite existing ideas to enhance the cooperation between Member States across all different areas of European security the Union is lacking sufficient power to provide security throughout all parts of own territory and stability in own neighbourhood. In fact, considering its low deterrence potential Europe’s security strongly relies on the conventional and nuclear power of the USA as most important partner. This lack of independence sends out clear signals to other actors that wish to use military force against EU boarders in pursuit of their own interests.
Political Unity

The ability to provide security in Europe requires a high degree of unity and strong common will on the political level. Europe can only be successful as long as it is acting along a common political position or speaking with one voice. Individual steps of member states will not have the power to prevail. On the other hand, unity is also a point of vulnerability. Other actors may on certain occasions “direct” hybrid measures with the particular intention to play off partners against each other. In this respect, the complex and very controversial political discussions on the common financial situation and the financial stability of single European states as well as the different positions on how to resolve the refugee problem provide a potentially rich “attack surface”.

Global Integration

Through the global economy, western society has become increasingly dependent on international flows of goods, services, human, and financial resources.

Ties are not limited on territory of EU Member States as shown by the dependencies of the Western economy on Russian oil deliveries through Belarus. Trading in all sectors, e.g. raw materials, infrastructure for Internet communication are organised and sourced worldwide. Europe is therefore extremely prone to disruption on its global interdependencies.

Open Society

The basic infrastructure like water and power supply, transportation networks (roads, railways, public transportation, air transport etc.), cultural institutions such as museums and theatres, sports-stadiums, shopping malls etc. builds the “technical backbone” of our social life. It belongs to the critical infrastructure as it is easy to attack with huge number of victims (“soft targets”) and as it has no “shield” to protect it and maintain “normal operations” during critical or conflict situations. The dramatic pictures and news on recent terrorist attacks in Brussels and Paris have proven that an open society is exposed to risks on a permanent basis and therefore extremely vulnerable.

Besides critical infrastructure, western societies are also extremely vulnerable given their plurality and religious diversity. As clearly demonstrated by Russia’s activities on Crimea and Ukraine, it is important to understand that destabilizing a country by addressing minorities can be more efficient than using conventional military forces.

Hybrid warfare and the role of deception and Information Warfare

Information warfare in history

It is very well known that concept of deception, or bluff, has been an integral part of warfare itself since ancient times. In our military history, we can find many examples of using various
forms of diversion, camouflage and disinformation campaigns, which played a crucial role in turning back the tides of war. Warlords and military commanders were often willing to sacrifice all possible resources to trick their adversary into believing that it was in fact in their favour to do a specific action, i.e. an action, which was not beneficial for the adversary himself, but for the originator of the deception. Furthermore, even on the lowest possible level of the military structure, the soldier fighting another soldier in hand-to-hand combat often struck with his right hand while feigning a strike with the left.

The first written record, which undoubtedly indicates the use of deception (not only) in a military context, is a statement from Sun Tzu’s military treatise called Art of War [15].

Although Sun Tzu’s concept of deception (as well as his work) is almost 2,500 years old, it is still considered to be a valid and fundamental foundation for many military doctrines currently taught at military academies throughout the world - because contrary to means of warfare, the principle always remains the same.

However, even though Sun Tzu was obviously the most famous military strategist when it comes to the use of deceptive means, there were many others who tried to develop his concept in accordance with the changing nature of warfare. The history has many examples; the Mongolian warlord Genghis Khan, who used specially trained units to spread rumours about the size and effectiveness of his army with the sole aim to frighten the opponent’s troops during the 13th century; Napoleon Bonaparte the French military commander and later Emperor, who was a huge and successful practitioner of a military tactic called strategic envelopment (i.e. small force distracts the enemy while a much larger force moves to attack from the rear or flank) as at the battle of Lodi in 1796; and last but not least general Edmund Allenby, whose agents spread false information about establishing their headquarters in a particular place in order to influence the movement of the adversary during the First World War.

Information warfare in the modern age

In the beginning of the 20th century, waging of extensive wars became more complex and so the invention of an effective deception plan on the tactical level became much more difficult. It was not an unusual scenario, that in the course of the world wars, both of which were so-called total wars, several allied commanders using different tactics shared the same goals as well as the same battlefield. It was due to their separate approaches to military planning and also imperfect communication means, that the use of deception on the tactical level declined significantly in this period (otherwise it could have had unexpected and undesirable effects). On the other hand, main deception planning shifted up to the strategic level (deception on the strategic level had been considered very uncommon until the period of world wars). Especially sophisticated was in this case the Soviet doctrine of Russian military deception code-named Maskirovka, which was developed in 1920s and included mainly concealment, imitation, deceit, denial and disinformation. This doctrine was referred to as “a complexity of measures, directed to mislead the enemy regarding the presence and disposition of forces”, but the latest version of the doctrine additionally includes “strategic, political and diplomatic means including manipulation of the
facts, situation and perceptions to affect the media and public/world opinion in order to achieve or facilitate tactical, strategic, national and international goals”.

As mentioned above, in the terms of modern warfare, the use of almost every form of deception is in fact common on the strategic level as well as, to a lesser extent, on the tactical one. According to NATO’s most recent definition, Deception, sometimes called “stratagem” is a complex art, which demands considerable effort, a high level of security and sound understanding of an adversary’s way of thinking, and which involves measures designed to mislead adversaries by manipulation, distortion or falsification. Within a deception plan, both information and traditional physical means and methods (camouflage, concealment, disguise, but also demonstrations and show of force) can be applied. While so-called traditional means have been pushed into the far background recently, use of various information means, e.g. tools associated with information warfare such as spreading of propaganda and disinformation has been experiencing an increase, primarily in connection with the rapid development of cyberspace.

Military and Political stratagems

At this point it is probably worth considering that a military stratagem to deceive the adversary is both understandable and acceptable however, a purely political stratagem intended to deceive one own’s population or to mislead the press would likely cause democratic governments in the EU "issues at home."

According to this definition, it is clear, that the whole concept of deception belongs to the sphere of information warfare.

The aim of information operations / warfare is to affect the will, understanding and capability of adversaries, potential advertisers and other approved targets / audiences.

To know the adversaries in particular their weaknesses in order to be able to manipulate them by these means becomes essential in information warfare. To achieve this aim a close connection and cooperation between the intelligence branch and the information branch is needed. On the other hand, our own weaknesses, when unknown by the adversary, become very important to protect. Likewise, should these weaknesses be discovered by the adversary, preventing the adversary exploiting them against us becomes very important. On the highest level, the weaknesses initially not known by any of the parties will be those that will prove to be the most dangerous once they are identified by our adversary on our side and likewise most favourable for us when we identify them on the adversaries’ side. Understanding the adversaries and our own weaknesses become essential in information warfare.

Information warfare types

There are many different definitions of information warfare, as shown below in Table 1, but in general, it can be described as a process of (i) protecting one’s own sources of strategic information on one hand and also (ii) denying, degrading, corrupting or destroying the adversary’s
sources of strategic information. It is divided into two categories: defensive information warfare (operational security) and offensive information warfare (electronic warfare, psychological operations, deception, physical attack and information attack).

<table>
<thead>
<tr>
<th>Effector</th>
<th>Outcome</th>
</tr>
</thead>
<tbody>
<tr>
<td>electronic warfare</td>
<td>jamming and spoofing radars and radio communication links</td>
</tr>
<tr>
<td>psychological operations</td>
<td>using information to weaken the adversary’s morale and break his will to resist</td>
</tr>
<tr>
<td>deception</td>
<td>employing (mainly) information means to confuse the adversary</td>
</tr>
<tr>
<td>physical attack</td>
<td>damaging or destroying the adversary’s means of processing strategic information</td>
</tr>
<tr>
<td>information attack</td>
<td>use of computer technology to electronically shut down, degrade, corrupt or destroy an adversary’s information systems</td>
</tr>
</tbody>
</table>

*Table 1: Description of Information warfare effectors and their intended effects.*

Although the concept of information warfare may sound quite new, the exact opposite is true, and there are in fact many indications that information warfare was the key element in winning the most notable conflicts in the 20th century (e.g. offensive information warfare used during the Second World War, which was based on tricking some of the axis leaders into believing that the invasion should have started in Calais instead of Normandy etc.). On the other hand, it is obvious that we cannot speak about “old-fashioned” information warfare any longer as there have been many changes concerning its methods and more importantly its extent and possibilities (especially in connection with the constant growth of information technologies). The changing nature of Information Warfare

Frankly speaking, recent forms of information warfare also remind us of the fact that modern warfare has, for the most part, started to lose its material nature. On one side, a physical attack followed by a complete destruction of the adversary’s significant infrastructure is still considered a great war success which can destabilise the adversary - even to the extent, that it literally allows his quick defeat. The problem is given the advanced state of information technology in the world today, a physical attack is in some cases no longer necessary. In an age, where all substantial players (governments, companies and individuals) rely heavily on electronic data storage, movement and communication, the key to the serious strategic harm resides in manipulation of information itself (i.e. destroying information, disrupting the complex structure of information and unauthorised use of information).

More importantly, there is also a question of development. It is true that effective using of information tools such as electronic warfare or information attack may prove very useful, especially in modern conflicts containing hybrid threats, but there is, of course, always an issue concerning the strong need for innovation of various capabilities associated with this kind of warfare. Since the information revolution started, constant improvement of information capabilities has literally become a question of survival in some areas. It is entirely possible to implement a new technology (or a method) one week only to realize the next that this technology (or the method) becomes obsolete. Sometimes, the process of improvement can be observed
as the modification of Red Queen’s race(1), where the one side must constantly keep refining its technology in order to stay even with the advances made in attack methods (e.g. when the computer system was firstly attacked, the attack technology was spread to involved computer manually – some time later, the attacker has placed the attack technology tools as part of the payload of a virus or worm, which also enables people or groups with less initial resources to launch an attack etc.). On the other hand, in case of psychological operations and deception, the approach is somewhat different. Instead of investments in new technologies, a strong focus on studying of the adversary’s behaviour is needed. Also, together with the rise of social networks, these in fact being powerful tools for their ability to put often-invisible pressure on public opinion, anew and more complex battlefield has been created.

Using Information Warfare to our advantage

To deal with the issue and the question “how to use information warfare’s levers to our advantage” is very difficult in this context, because from the point of view of any NATO state, no offensive information attack is allowed during peacetime. It is possible to perform this kind of attack in a state of war, of course, but then there is a problem with hybrid warfare itself, which covers the period when no war is formally declared, and today wars are very often not declared or indeed declarable if there is no recognised Nation State adversary with which to serve an official “war declaration’’. That is why the highest priority should be the development of the defensive aspect of information warfare, which has been underestimated lately. The main goal of this development/improvement should be the creation of a self-sufficient working framework with the ability to prevent or counter hostile approaches coming from a potential adversary (for this matter, possible opponent approaches must be understood and analysed).

Information tools and techniques

There are many tools of information warfare, which are based on deception and psychological operations and targeted at harming the opponent, but in connection with recent hybrid threats, well-managed propaganda seems to be definitely the most dangerous of them all.

In general, propaganda is described as a form of “seemingly harmless” communication, which is aimed at promoting or demoting certain views, perceptions or agendas. Its deliberateness and a strong emphasis on manipulation with the target audience distinguishes propaganda from ordinary advertisement or education. It includes both, lying to the audience directly (such as during the Second World War) or presenting facts selectively in order to form certain associations

---

(1) “The Red Queen’s race is an incident that appears in Lewis Carroll’s Through the Looking-Glass and involves the Red Queen, a representation of a Queen in chess, and Alice constantly running but remaining in the same spot. "Well, in our country," said Alice, still panting a little, "you’d generally get to somewhere else – if you run very fast for a long time, as we’ve been doing."

“A slow sort of country!” said the Queen. “Now, here, you see, it takes all the running you can do, to keep in the same place. If you want to get somewhere else, you must run at least twice as fast as that!” https://en.wikipedia.org/wiki/Red_Queen%27s_race
or conclusions (Russian propaganda used before the annexation of Crimea). When used during hybrid conflicts, propaganda campaigns often follow some sort of higher strategic pattern of transmission to indoctrinate the targeted group.

The main problem connected to this concept is that propaganda is not unlawful - of course there are some measures developed to counter propaganda, but as recent hybrid conflicts show, it is far from enough in a society, where social media and other forms of internet-based communication create huge opportunities for radicalization. Even though people in democracies tend to claim unlimited freedom of speech without any propagandistic influence, propaganda is to democracy what violence is to totalitarianism as Noah Chomsky notes, so it is important to realize that governmental institutions and other major institutions (especially media), which are in fact susceptible to propaganda, must be constantly maintained to avoid propaganda.

The importance of propaganda in the modern face of conflict is easily illustrated with groups like ISIL, for whom propaganda is one of the core methods with which they enact operations. These groups project multiple images of themselves all at once, depending on the recipient. From confidants that extol their virtues over social media, to images of a strong and well-trained military organization, which tends to circulate from their media releases. But groups like ISIL, Hezbollah and similar non-state actors are not the sole users of similar tactics, even though this may have been historically accurate. Propaganda in virtually every media space has been an intrinsic part of the Russian annexation of Crimea, both before and during any actions performed.

The sheer scope of this is staggering and the utilization of various media platforms somewhat astounding ranging from civilians “virtually indistinguishable troll soldiers” to reputable media companies controlled by Moscow (e.g. the most famous channel “Russia Today”, whose existence is directly sponsored by the Russian government etc.). While the quality of much of this content is questionable at best and the West often ridicules it, the constant barrage and mass of it makes it complex to completely negate. Rightly, NATO Supreme Allied Commander General Philip Breedlove has called this Russian approach a veritable modern “Blitzkrieg” of information warfare. Noah Chomsky summarised this in his 1993 reflection:

“In a totalitarian state no matter what people think, because the government can control it by force using batons. But when you cannot control people by force, you have to control what people think, and the typical way to do this is through propaganda (manufacture of consent, creation of necessary illusions), marginalizing the general public or reducing it to some form of apathy”

There are some aspects that we could consider as weaknesses such as the EU’s Legal framework, which obviously prevents any EU member, either jointly or in cooperation, from using many of

(2) The Islamic State of Iraq and the Levant and/or the Islamic State of Iraq and Syria (ISIS)
the hybrid tactics as they are considered to be in contravention of National and International Law or simply not acceptable “behaviours’, but we need to consider the ESS and the reasons why Russia has come to tackle International relationships differently.

Russia openly stated through its president in February 2007 in his Munich Speech at the 43rd Munich Conference on Security Policy that the model of international relations would not be accepted and that Russia would implement its own independent foreign policy in pursuit of its geopolitical interest.

The first page of the ESS states, “A Secure Europe in a better world“ and under the heading of “Building Security in our neighbourhood“ there follows, “The integration of acceding states increases our security but also brings the EU closer to troubled areas. Our task is to promote a ring of well governed countries to the East of the European Union and on the borders of the Mediterranean with whom we can enjoy close and cooperative relations“ and shortly afterwards “We should now take a stronger and more active interest in the problems of the Southern Caucasus, which will in due course also be a neighbouring region."

Reading these statements from an EU member state point of view suggest that this strategy is purely about working with non-EU States in Eastern Europe however, a resurgent Russia may see this as a statement of expansion into areas of interest to Russia, thus puts into context President Putin’s statements in Munich declaration. It is naive to think that our goals as expressed into European Security Strategy, although desirable for many, cannot be seen from Russia as anything other than an aggressive policy against their geopolitical interest. Accordingly, the lack of empathy on how EU policy may be seen by others and more importantly, the lack of prescience shown by EU and its inability to remember the European tensions and misunderstandings over the last 300 hundred years is remarkable. As Jorge Santayana, philosopher and novelist, expressed it:

“Aquellos que no pueden recordar el pasado estan condenados a repetirlo” (“Those who cannot remember the past are condemned to repeat it”).

George Santayana (1905) Reason in Common Sense, p. 284, volume 1 of The Life of Reason

Warfare and Countermeasures

The answer to the question regarding right countermeasures is, of course, a very complicated one. Perhaps, a source of inspiration for possible countermeasures might be found in the Swedish doctrine of Total Defence, which also included provisions against information misuse. Headed by the “Styrelsen foer psykoloeist foersvar’ (Board for Psychological Defence), the Swedish established a civilian body – an agency tasked with combating dangerous external propaganda, subversion and disinformation during the Cold War (tasks such as protecting the country’s main television and radio transmission sites, researching and carrying out public opinion surveys on topics such as the population’s willingness to defend their country, their trust in public officials, tracking and analysing the propaganda and disinformation transmitted
by external actors as well as providing information on security and defence policies to domestic audiences etc.). Sweden also established very sophisticated system that aimed to educate the population regarding the pitfalls of external propaganda, especially through acts of wide public outreach, leaflets distributed through telephone registries etc.

“All warfare is based on deception. Hence, when we are able to attack, we must seem unable. When using our forces, we must appear inactive. When we are near, we must make enemy believe we are far away. When far away, we must make him believe we are near.”

Although quite controversial, there is also a debate concerning possibilities of limiting, controlling or influencing the national (European) media’s ownership in connection with investors from countries, which do not belong to NATO (esp. Russia or China). In the sense of fighting propaganda, information warfare as well as maintaining democratic (European) values such as freedom of speech (including freedom of opinion and expression), the independence of media must be maintained at all costs—quite simply because the media are the most important tools used to form the major public opinion nowadays. On the other side, there are also “social media”, which despite the fact, that are still part of the overall media network, are accessible by almost everyone and cannot be controlled or limited by any acceptable means or methods.

**Methodology**

**Committee 2 approach**

Our work detailed in the above sections led us to the conclusion that hybrid warfare is a dynamic, evolving process comprising a number of complex, interacting and often interdependent factors. Therefore we decided to build a high level model and risk based assessment process in order to identify and qualify EU vulnerabilities to hybrid warfare and develop possible avenues for the EU to both counter use of hybrid warfare as well as conduct it within its own legal and moral context.

Our basic approach is show below in Figure 1 and in more detail in Annex B: Methodological Approach. Figure 1 shows a simple 5 step process:
Committee 2 Hybrid Conflict Methodology Development

✓ Conduct a pragmatic analysis of a range of hybrid warfare examples;
✓ Extract common and unique factors from these examples and use them to construct a high level and simple dynamic model;
✓ “Run’ the paper based so we could assess and judge the benefits and disbenefits of using multiple hybrid effects simultaneously;
✓ Feed these results back in to the ‘table of effectors’ to generate vulnerabilities and counters
✓ Reiterate this process to refine our conclusions.

Scenarios

We chose five scenarios from which to develop the common and unique factors as tabulated below in Table 2: Scenario synopsis. Details can be found at Annex C: Scenario background.

<table>
<thead>
<tr>
<th>Scenario</th>
<th>Summary</th>
</tr>
</thead>
<tbody>
<tr>
<td>Israel vs Hezbollah in 2006</td>
<td>Prototype Hybrid Warfare. 34-day military conflict with use of: conventional arsenal, irregular forces, guerrilla tactics, psychological warfare, terrorism, criminal activities, and the support by Iranian Revolutionary Guards to Hezbollah.</td>
</tr>
</tbody>
</table>
Table 2: Scenario synopsis.

Hybrid factors, their effectors and outcomes

From these scenarios we distilled out the common and unique factors, their underlying effectors and the potential outcomes as tabulated below in Table 3: Hybrid warfare effectors and outcomes.
Terrorism  |  Assassination  |  Provoke Fear  |  Provoke Retaliation  
Terrorist Attacks (not cyber)  |  Cause Casualties  |  Damage/Destroy Infrastructure  
Weapons of Mass Destruction (WMDs)  |  Increase Publicity/Wider Awareness for Cause  |  Provoke "repressive" measures  
Terrorist Information Warfare (cyber)  |  Provoke Censorship  |  Increase Recruitment/Funding  |  Increase Radicalisation  |  Damage/Destroy Infrastructure  |  Increase Publicity/Wider Awareness for Cause  
Military Unconventional  |  WMD (Chemical & Biological only)  |  Unacceptable under 1992 CWC and 1972 BTWC  
Nuclear Deterrent Capabilities  |  Provide Nuclear Deterrence  
Special Forces  |  Provide special operations  
Militias  |  Provoke disorders  

Figure 2: Hybrid Warfare High Level Dynamic Model.
Table 3: Hybrid warfare effectors and outcomes.

<table>
<thead>
<tr>
<th>Military Conventional</th>
<th>Land Capabilities</th>
<th>Project Forces (land military operation)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Defend the Nation</td>
</tr>
<tr>
<td></td>
<td>Air Capabilities</td>
<td>Support Allies</td>
</tr>
<tr>
<td></td>
<td>Maritime Capabilities</td>
<td>Support International Operations</td>
</tr>
<tr>
<td></td>
<td>Space Capabilities</td>
<td>Enforce International Resolutions</td>
</tr>
<tr>
<td></td>
<td>Cyber Capabilities</td>
<td>Support International Treaties (Bi and Multi-lateral)</td>
</tr>
<tr>
<td>Economics</td>
<td>Basic food/water</td>
<td>Deny access to basic food/water</td>
</tr>
<tr>
<td></td>
<td>Energy</td>
<td>Deny access to Energy supplies</td>
</tr>
<tr>
<td></td>
<td>Internet</td>
<td>Provide disinformation/propaganda/counter Information Warfare</td>
</tr>
<tr>
<td></td>
<td>Law</td>
<td>Support International Institutions/Trade Agreements</td>
</tr>
<tr>
<td></td>
<td>Commerce</td>
<td>Access to internal and international markets</td>
</tr>
<tr>
<td>Political / Diplomatic</td>
<td>Gunboat Diplomacy</td>
<td>Support National Policies</td>
</tr>
<tr>
<td></td>
<td>Intelligence</td>
<td>Support National Industries</td>
</tr>
<tr>
<td></td>
<td>Law</td>
<td>Support Allies</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Support International Institutions</td>
</tr>
<tr>
<td>Society</td>
<td>National &quot;norms'</td>
<td>Provide own viewpoint and counter inform-</td>
</tr>
<tr>
<td></td>
<td></td>
<td>mation</td>
</tr>
<tr>
<td></td>
<td>Free Media</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Social Media</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Internet</td>
<td></td>
</tr>
</tbody>
</table>

Modelling Hybrid Warfare using System Dynamics (SD)

Committee 2 considered that SD might be a useful methodology to apply its set question above given the complexity of hybrid warfare and the dynamic nature of how each of the components interact and contribute to observed behaviour of the “system”.

The model is shown below in Figure 2 and reproduced in full at Annex D: The System Dynamics Model and theory along with a full description of the methodology and how it works. The “heart” of the model is based around the concept that the actors are deploying hybrid effectors in an uncertain, changing environment in which no one has perfect or timely information, to not only achieve their own strategic goals whilst minimising their adversaries attempts to do the same but trying to minimise the disbenefits that may accrue as they use effectors that are out with the accepted “norms” or that their success is solidifying support against them.

The “smiley’s simply illustrate the “for” or “against’ flows within the model. When using the model it’s probably best to envision two or more of these models in operation simultaneously, each modelling one particular effector but all feeding into a common and shared “heart”.
Model Conclusions

The risk based assessment

The Committee characterised potential actors into one of three groups: “EU’, “Other States’ and “Terrorists’. We recognise that is an oversimplification but meant that the analysis could be completed within the allocated session time.

Each hybrid effector was then scored using a simple weighting system. This system uses “−” and “+” signs to indicate the likelihood of use where a double “−” indicates no wish to use and a double “+++” a strong desire to use. Each hybrid effector was then scored against each actor taking into account availability of the effector, likelihood of use, intent of use and desired and potential outcomes.

The results shown below in Table 4 and fully detailed in Annex D: Hybrid Risk Assessment Methodology Results and are broadly in line with our expectations. For example, we couldn’t foresee any circumstances where the EU would threaten support or directly conduct terrorist attack, assassinations or use Chemical, Biological or Radiological Weapons to achieve its aims, whereas a number of other State or Terrorist actors would have no such qualms.

Similarly, both the EU and other Nation States have the whole range of conventional military forces in such a scale and capability that can’t be matched directly by small States or terrorist actors. However, as discussed below in section Political Unity the use of armed force and reaching a timely consensus gives rise to a number of political and military command & control issues within member States that other State actors may not share.

The use of International law and economic power gives the EU some major advantages and levers at its disposal, assuming of course that the political will is present within member States.
<table>
<thead>
<tr>
<th>Hybrid Factors</th>
<th>Hybrid Effector</th>
<th>Outcome / Reasoning</th>
<th>Likelihood of Hybrid Effectors being used by Hybrid Actors</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>EU</td>
</tr>
<tr>
<td>Terrorism</td>
<td>Assassination</td>
<td>Provoke Fear</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>Terrorist Attacks (not cyber)</td>
<td>Provoke Retaliation</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Cause Casualties</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Damage/Destroy</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>WMDs</td>
<td>Increase Publicity/Wider Awareness for Cause</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>Terrorist Information Warfare (cyber)</td>
<td>Provoke 'repressive' measures</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Provoke Censorship</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Increase Recruitment</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Increase Radicalisation</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Damage/Destroy</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Increase Publicity/Wider Awareness for Cause</td>
<td>-</td>
</tr>
<tr>
<td>Military Unconventional</td>
<td>WMD (Chemical &amp; Biological only)</td>
<td>Unacceptable under 1992 CWC and 1972 BTWC</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>Nuclear Deterrent Capabilities</td>
<td>Provide Nuclear Deterrence</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>Special Forces</td>
<td>Provide special operations</td>
<td>++</td>
</tr>
<tr>
<td></td>
<td>Militias</td>
<td>Provoke disorders</td>
<td>-</td>
</tr>
<tr>
<td>Military Conventional</td>
<td>Land Capabilities</td>
<td>Project Forces (land military operation)</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>Air Capabilities</td>
<td>Support Allies</td>
<td>++</td>
</tr>
<tr>
<td></td>
<td>Maritime Capabilities</td>
<td>Support International Operations</td>
<td>++</td>
</tr>
<tr>
<td></td>
<td>Space Capabilities</td>
<td>Enforce International Resolutions</td>
<td>++</td>
</tr>
<tr>
<td></td>
<td>Cyber Capabilities</td>
<td>Support International Treaties (Bi and Multi-lateral)</td>
<td>++</td>
</tr>
<tr>
<td>Economics</td>
<td>Basic food/water</td>
<td>Deny access to basic food/water</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>Energy</td>
<td>Deny access to Energy supplies</td>
<td>+</td>
</tr>
<tr>
<td></td>
<td>Internet</td>
<td>Provide disinformation/propaganda</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>Law</td>
<td>Support International Institutions/Trade Agreements</td>
<td>++</td>
</tr>
<tr>
<td></td>
<td>Commerce</td>
<td>Access to internal and international markets</td>
<td>++</td>
</tr>
</tbody>
</table>

Table 4: Hybrid Effectors and their potential use by Actors.

The risk based assessment and Capability v’s Vulnerability

After assessing the likelihood of use we took a further step and assessed both the EU’s potential vulnerability to these effectors and actors as well as the EU’s ability to wield such effectors against other actors. The results are tabulated in Table 5 below and the complete data set is presented in Annex E: Hybrid Risk Assessment Methodology Results.
### Table 5: The EU strengths and vulnerabilities in Hybrid warfare.

In this case we used a numerical scoring system ranging from -4 (non-existent) to 4 (internationally excellent) to assess each effector. Interestingly as detailed below, the EU like all advanced ‘States’ is particularly vulnerable to attacks against basic food, water and electrical infrastructure as well as disinformation campaigns waged on the world wide web. Many of the member states have significant military capabilities but wielding these national capabilities within a unified EU Command and Control environment will be challenging.
Hybrid Warfare and Information

Further development of advanced information technologies:

Although investments into new information technologies are often considered very expensive, they are certainly needed; otherwise, the probability of intercepting and disrupting the most vital and critical sources of strategic information by the adversary increases substantially.

Improving of technological capabilities by:

- Creating mapping programs that find points of vulnerability in the Internet;
- Developing of encryption based validation and verification systems;
- Developing new effective programs, virus detectors, firewalls etc.;
- Use of highly skilled teams of security testers to test vulnerabilities (inside or outside organizations);
- Distributing services and expertise, so that critical services can absorb local damage;
- Reducing the reliance on hierarchical power structures, with the accompanying levels of secrets. As Brin [18] reflects:

"A huge percentage of governments still operate on the pyramidal power structure, when power and authority flow from the top down – the entire branch of the military is hierarchical in nature – this is the root of the military’s ultimate ineffectiveness in dealing with a networked threat".

Information-based deterrence:

Although an overt information warfare campaign against the potential adversary is highly questionable, concept of information-based deterrence is based on manipulating the potential adversary during peacetime or a crisis in order to prevent him from ever attacking; it is definitely not a new concept (it was used many times in the past, often in connection with diplomacy), but technological growth and existence of the Internet itself (including social media) are surely able to increase its scope. According to Brian Nichiporuk [19], this kind of deterrence can be done in three ways:

- Turning international opinion against the aggressor;
- Altering his perception of the military correlation of forces in theatre and;
- Fostering inability in his country.
Improving C4ISR capabilities/counter C4ISR capabilities:

The counter C4ISR campaign involves improving own information warfare tools and techniques to be able to attack adversary sensors and communication assets; increasing readiness and answerability.

Supporting the international discussion on this matter/international cooperation:

Even though it is very difficult to say what future wars, including hybrid threats will look like, one thing is now certain – soldiers who will fight in these wars will be relying heavily on advanced information technologies; even now, it is sometimes difficult to imagine that both advanced missile systems and soldier’s computer-aided gear such as weapon-sighting system, are based on information technologies; the second thing is that in connection with hybrid threats, warlike conflicts are no longer exclusive domains of state actors, or guerrilla groups fighting an oppressive government, but also result of actions of loosely based organized groups, whose members can conduct information warfare on a vast array of targets; the complex and interconnected world allows attacks to come from nearly anywhere (and it is possible to use this kind of attacks in combination with conventional means).

Hybrid warfare: the internet and cyberspace

Many people today are talking about the impact of information technology on the world. They are discussing how business, the economy, education, and even personal relationships are being affected by the onset of the information age. It should come as no surprise, then, that people are also talking about how technology is impacting the way we engage in one of our oldest traditions - war. The term "information warfare" has been in use for a number of years now, intended to represent whatever warfare is becoming in the information-centric 21st century. Unfortunately, though, many people use this term without really knowing what it means. In an effort to make progress toward a common definition, this section presents one possibility and expands on it by discussing the weapons, strategies, and countermeasures involved in "information warfare", as defined.

Defining Information Warfare (IW)

If there were a single, obvious definition of information warfare, someone would have already written it down. The fact that no one has done so indicates that perhaps no simple definition exists. Those in the IW community have come to agree that information warfare is not a single, simple thing, that it has many complex dimensions.

Unfortunately, agreeing on the fact that IW has many dimensions does little to further our understanding of it. Luckily, opinions are diverging on some things but converging on others. For the purpose of this discussion, we talk about information warfare as a class of techniques, including collection, transport, protection, denial, disturbance, and degradation of information, by which one maintains an advantage over one’s adversaries. The above definition can certainly be applied in any competitive situation, public or private, civilian or military.
Weapons of Information Warfare

Having established a definition of information warfare, the next logical question is - what do we need to be involved in it? Specifically, what are the weapons of information warfare? To answer this question, we look at each of the techniques mentioned above and give a brief overview of the most common weapons used to achieve them.

Information Collection

Information collection is included as part of information warfare because the information revolution implies the rise of a mode of warfare in which the side that knows more, and faster, will enjoy decisive advantages. The idea is that the more information one has, the higher his/her situational awareness, which leads to better battle plans and, hopefully, better outcomes. In information warfare, information collection is much less dangerous and much more complete because reconnaissance and surveillance technologies can be used to infiltrate situations and gather accurate information with minimal loss of fidelity.

Information Transport

Collecting a large amount of comprehensive information is certainly good practice, but collection is of little value if the information sits in a storage facility, unused. As such, the ability to transport information into the hands of those who need it, in a timely manner, is another essential aspect of information warfare. The tools used in this domain are not exactly weapons, but rather civilian technologies put to use in military situations. The most important of these tools is communication infrastructure, composed of networks of computers, routers, telephone lines, fiber optic cable, telephones, televisions, radios, and other data transport technologies and protocols. Without these technologies, the ability to transport information in the real-time fashion required by today’s standards would be impossible.

The new technology may also provide greater "topsight", a central understanding of the big picture that enhances the management of complexity.

Information Protection

One of the most broadly agreed upon aspects of information warfare is the need to minimize the amount of information to which your opponent has access. A large part of this is protecting the information you have from capture by the other side. The weapons used to protect the security of our information fall into two classes. First are those technologies that physically protect our vital data storage facilities, computers, and transport mechanisms, including intrusion prevention mechanisms such as locks and fingerprint scans. Second, and perhaps more important, are technologies that prevent bits from being seen and intercepted by the enemy. This certainly includes basic computer security technologies such as passwords, as well as more sophisticated technologies like encryption.
**Information Manipulation**

Information manipulation in the context of information warfare is the alteration of information with intent to distort the opponent’s picture of reality. This can be done using a number of technologies, including computer software for editing text, graphics, video, audio, and other information transport forms. Design of the manipulated data is usually done manually so those in command have control over what picture is being presented to the enemy, but the aforementioned technologies are commonly used to make the physical manipulation process faster once content has been decided.

**Information Disturbance, Degradation, and Denial**

The final aspects of information warfare, according to earlier definition, are disturbance, degradation, and denial. All three techniques are means to the same general end - preventing the enemy from getting complete, correct information. Because of their similarity, many of the same weapons are used to achieve one or more of the goals. As such, it makes sense to discuss them together. Some of the more popular weapons used to wage these types of information warfare are spoofing, noise introduction, jamming, and overloading.

Spoofing is a technique used to degrade the quality of the information being sent to the enemy. The enemy’s flow of information is disturbed by the introduction of a "spoof", or fake message, into that flow. The technique works because it allows you to provide false information to the targeted competitor’s collection systems to induce this organization to make bad decisions based upon this faulty information.

Another way to disturb the information being received by one’s opponent is to introduce noise into the frequency they are using. Background noise makes it difficult for the enemy to separate the actual message from the noise. This is a particularly useful technique if the enemy is using forms of wireless communication, since those frequencies can be tapped without having to actually link into a physical network of cables.

Jamming is a technique used to achieve denial that involves intercepting signals sent between two communications links or between a sensor and a link. The signal is intercepted, then "jammed" or stopped from further progress toward its intended destination. In most cases, that same signal is stored by the captor as intelligence information and used to determine the enemy’s view of its own position in the contest.

Finally, overloading is technique used to deny information to the enemy in both military and civilian settings. By sending a volume of data to the enemy’s communication system that is too large for it to handle, one causes a crash or severe degradation of the system’s ability to deliver information. The system is so busy dealing with the overload, it is unable to deliver the essential information to those who need it. This tactic is referred to as a "denial of service" attack, and has been proven both easy and effective.
Defending Against Information Warfare

The techniques and “effectors” listed above certainly have the potential to cause severe damage to an information dependent military operation. How do we defend ourselves, then? There are several ways, many of which employ the same techniques we use to attack others. The remainder of this section examines available countermeasures for each of the dimensions of information warfare.

**Information Collection**

To defend against information collection attacks is to prevent our enemies from assembling information about us and about the conflict situation. Doing this involves protecting our own information from interception and preventing information from getting to the enemy’s collection facilities. The available countermeasures for defending against information collection, then, are the same weapons defined earlier for use in protection, disturbance, degradation, and denial attacks. Specifically, the use of encryption, spoofing, noise introduction, jamming, and overloading are particularly useful for keeping the enemy’s information collection to a minimum.

**Information Transport**

Because information transportation is heavily dependent upon infrastructure, the most effective countermeasure for preventing transport is the destruction of the enemy’s infrastructure. Attacking an enemy’s infrastructure as a countermeasure to information transport can not only be particularly easy, but can also have far-reaching effects on their entire information system.

**Information Protection**

To counteract enemy attempts to protect their own information supply, we must be able to get around their protection mechanisms. As was mentioned earlier, the primary technological effector for protecting one’s own information is encryption. Unfortunately recent increases in the sophistication of cryptography have made countermeasures very difficult to execute, notwithstanding advances in quantum computing technology and the potential for rapid “crypto cracking. What this means for those wishing to counter information protection is that their efforts will eventually become futile. Until then, though, attempts to break codes using powerful computers will most likely yield the best results.

Although it is the most effective, cryptography is not the only tool for information protection. In fact, passwords are a much more widely used technique for protecting information systems from unauthorized access. Unfortunately, however, password systems are dependent on humans to keep track of and enter codes, which open them up to significant vulnerability. If it is possible to get a physical presence near the system or those who use it, obtaining or guessing passwords can be amazingly easy, and is a very effective means for getting access to protected information.
Information Manipulation

Once an enemy has information, there is little anyone can do to prevent them from manipulating it. In light of that, there are really only two countermeasures available to defend against this kind of attack. First, one can work to prevent the enemy from intercepting information in the first place. Techniques for information protection are most effective here, since they keep the enemy from either getting access to or being able to understand the information as originally transmitted.

The second, and perhaps more crucial, key in defending against data manipulation is to prevent the altered data from being re-introduced into the flow of real information. Luckily, there are several techniques for doing this, the most common of which is redundancy. By gathering the same information from multiple, redundant sources, you increase the likelihood that the correct information will get through. Even if the enemy is successful at corrupting that data on one communication line, you will easily detect the bad data because it differs from the picture painted by the rest of your sources.

Information Disturbance, Degradation, and Denial

Defending against information disturbance, degradation, and denial requires the use of many of the countermeasures already mentioned. Any of the weapons for mounting these types of attack require access to enemy communication channels, so information protection mechanisms and redundant channels can be effective in maintaining some lines of communication that are not affected by would-be attackers. There are also several techniques available that are specifically designed to counteract the weapons described for performing disturbance, degradation, and denial attacks (frequency-hopping, spread-spectrum, and code-division multiple access (CDMA) technologies, digital compression techniques coupled with signal redundancy). These techniques, and the thousands of others currently under development at research sites all over the world, make it easier every day to recover from attempts to mangle and block information as it travels to its intended destination.

Cyber warfare

Cyberspace can be absolutely considered part of information world. So, cyber warfare can be defined as "attacking and defending information and computer networks in cyberspace, as well as denying an adversary’s ability to do the same".

But how do we define thresholds in cyberspace? It is useful to consider three dimensions: confidentiality, integrity, and availability of data. A few key cases help unpack these concepts.

Confidentiality is the principle that sensitive data should be kept out of the wrong hands, and breaches of confidentiality are perhaps the most common form of cyber-attack. Take the widespread accusations that the Chinese hacked Lockheed systems and stole blueprints for the new F-35 aircraft. This attack produced a tangible strategic loss for the United States - and for allies
who buy the F-35. It provided the Chinese with not only the information to build a competitor aircraft, but also information to help defend against such an aircraft. Chinese responsibility for the incursion is widely acknowledged.

The second principle, availability, is just what the word says: The concept that data must be available to users. The DDoS campaign against Estonia is a prime example of an attack that compromises availability. The attack crippled Estonia’s servers and routers, temporarily disconnecting the country from the Internet. Estonia responded by blocking global access to websites hosted in Estonia, blocking all Internet traffic originating in Russia, and requesting support from its NATO allies. NATO quickly dispatched a group of experts akin to a forensics team, but no counter attack, physical or cyber took place.

So why didn’t these two cyber events trigger a visible military response from NATO or NATO members? There are a number of factors in play. At a fundamental level we can look at the actors involved and the losses incurred. Russia and China are both emerging global powers with formidable cyber and physical force, and the cost of expanding ongoing political conflicts to the military level is simply too high. But the rationale extends further. Though some may disagree, these attacks alone do not constitute acts of war. They qualify as espionage, sabotage, and crime - they affect data confidentiality and availability, but not our third key principle: integrity. Also the concept of data integrity is important. Data can be manipulated; integrity is the concept that data remains valid, or unchanged. We can conceive of a cyber-weapon that infects an industrial control system, alters the data that governs the system, and causes a leak at a chemical plant or shuts down an electrical grid. The Stuxnet virus, which the United States and Israel reportedly deployed to sabotage an Iranian nuclear facility, is an example of a capability to infect and manipulate data on an industrial control system. However, the attack sought only to damage a facility’s capacity, not to induce human casualties. A sophisticated malware could conceivably be deployed in the future in a densely populated area where it threatens human life and not just that of an industrial system.

But what kind of actor would carry out such an attack? The chances of traditional NATO adversaries such as Russia or China engaging in this type of activity during peacetime are virtually nil. Indeed, any country that adheres to general “Just war” principles such as proportionality and distinction is unlikely to carry out such an attack, even during wartime. An attack on a nuclear or chemical facility in a populated area could yield an unacceptably high level of collateral damage, including civilian casualties. Data manipulation weapons are notoriously difficult to control if deployed remotely and can spread to infect unintended systems, including the attacker's own. The source of such an attack would have to be an international actor that does not adhere to just war.

Undoubtedly, these actors do exist, but extremist groups such as Islamic State and al Qaeda have access to much simpler and cheaper ways of inducing mass casualties, undercutting their incentive to develop and deploy greater cyber capabilities. This is not to say that an attack of this sort is impossible, but as King’s College professor Thomas Rid is quick to point out, an attack like this may be unrealistic at this point in time.
It is becoming increasingly clear that few cyber attacks are acts of war. A small number of cyber attacks involve data manipulation, and even fewer pose militaristic threats. Instead, so-called attacks are most often on availability and confidentiality and should be treated as crime. NATO is not a crime fighting organization; it is a military alliance. What NATO should do now is clarify its own role in cyber conflict.

Political context

An important condition in establishing a hybrid strategy is getting a clear picture of Europe’s vulnerabilities as discussed above. Since the situation in each of the European states are quite different, it is necessary to take into account the context of the specific countries to get an overview of Europe’s vulnerabilities.

A country’s vulnerability and also strengths is closely linked to its history and its present condition. Some are old democracies, some are young. Some nations are member of NATO, others are in Partnership for Peace (PfP). Some are members of European Defence Agency (EDA), and there are several bilateral collaborations. Aspects as the economic state of the nation, quality of the public debate, level of education and level of digitalization must be taken into account. The same goes for the country’s geographic position since it leads to different exposure to external threats, migration routes and migrants as well as conventional threats.

The past has shown us that if there is a problem then each member state of the European Union (EU) can behave in its own interests rather than as an interconnected aspect of a larger “Union”. The dilemma for the different governments are, that it has to take care of its own population and at the same time act in accordance to the Treaties and “agreed norms” of the EU. And in most cases history shows, that the national advantage is often the “winner”.

An example of this is the handling of refugees, where nearly all EU member state have approached this complex issue in different ways and from different viewpoints. Maintaining social cohesion and stability is often the priority for National governments and many attempt to restrict the number of refugees that they “will take in”. This even though it meant not acting according to the Dublin-agreements. As such these types of issues are likely to widen rifts within the EU. The lack of a truly cohesive united political worldview within the EU is one of the reasons why it at the moment is nearly impossible to lever hybrid warfare to Europe’s advantage. If you act in 28 different ways it is rather easy for other actors to make use of hybrid warfare and to undermine any combined EU efforts. Within the EU there is democracy, and as mentioned earlier some states have lived as democratic societies for centuries whereas for other members democracy is still in its infancy after just a few decades. But in general the populations are used to being “free”, to expect the right to free debate and express political and religious beliefs. Also they are used to have a free press. Even though the core items of “European way of Life” is written in the Treaty on the EU, there is a lack of common understanding and agreement on what the “European way of Life” comprises of. Every country has its own understanding and the lack of agreement makes it harder to protect the EU as a broader institution.
Digitalization is part of our daily lives. Anyone can access information in our 24/7 culture and 24 hour news cycle thanks to the ubiquitous “world wide web. This could help to show everybody who has in interest the potential for the “European way of Life”. But to do this EU would have to define this kind of information and each member state then have to agree and implement this approach. On the other hand, this kind of transparency results in vulnerability and a bigger “attack surface”, since transparency and “big data collection’ comes with a duty to protect information and information-infrastructure. Security is therefore much more complex and expensive to achieve.

**In conclusion**

The EU has the capacity to use hybrid warfare effectors to its advantage whilst operating within the spirit of EU and International treaties and “accepted norms’. The EU's openness, democratic foundations and the fact it comprises 28 different member States which makes timely decision making time consuming, and each member state has complex geographical boundaries makes the EU particularly vulnerable to hybrid warfare.

In order to address the complexities of hybrid warfare Committee 2 has developed a risk based analysis. This approach is supported by the development and use of a high level dynamic model to assess the benefits and disbenefits, vulnerabilities and potential levers relating to Hybrid Warfare. This approach has developed a basic tool set with which decision makers and analysts can model actions and outcomes before making any commitments to one or more courses of action. This tool set will require further refining.
Main references

18. Brin
19. Nichiporuk, B.,
Annex A: Treaty Text Excerpts

Article 2 (UN Charter Excerpt)
The Organization and its Members, in pursuit of the Purposes stated in Article 1, shall act in accordance with the following Principles.

1. The Organization is based on the principle of the sovereign equality of all its Members.
4. All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations.

Article 5 (NATO Treaty)
The Parties agree that an armed attack against one or more of them in Europe or North America shall be considered an attack against them all and consequently they agree that, if such an armed attack occurs, each of them, in exercise of the right of individual or collective self-defence recognised by Article 51 of the Charter of the United Nations, will assist the Party or Parties so attacked by taking forthwith, individually and in concert with the other Parties, such action as it deems necessary, including the use of armed force, to restore and maintain the security of the North Atlantic area.

Any such armed attack and all measures taken as a result thereof shall immediately be reported to the Security Council. Such measures shall be terminated when the Security Council has taken the measures necessary to restore and maintain international peace and security.

Article 4, The Lisbon Treaty.
1. In accordance with Article 5, competences not conferred upon the Union in the Treaties remain with the Member States.

2. The Union shall respect the equality of Member States before the Treaties as well as their national identities, inherent in their fundamental structures, political and constitutional, inclusive of regional and local self-government. It shall respect their essential State functions, including ensuring the territorial integrity of the State, maintaining law and order and safeguarding national security. In particular, national security remains the sole responsibility of each Member State.

3. Pursuant to the principle of sincere cooperation, the Union and the Member States shall, in full mutual respect, assist each other in carrying out tasks which flow from the Treaties.

The Member States shall take any appropriate measure, general or particular, to ensure fulfilment of the obligations arising out of the Treaties or resulting from the acts of the institutions of the Union.

The Member States shall facilitate the achievement of the Union’s tasks and refrain from any measure which could jeopardise the attainment of the Union’s objectives.
Committee 2 Hybrid Conflict Methodology Development

Annex B: Methodological Approach

Historical Analysis of previous uses of Hybrid Effectors

Identification & Analysis of common and unique effectors

Development of a High Level System Dynamics Model

Analysis of ‘blended’ effectors and strategic outcomes

Development of new ‘predictive’ scenario - “Where will Hybrid warfare occur next?”
Annex C: Scenario background

Israel vs Hezbollah in 2006

2006: Rocket attacks on Israel

12/07/06: Hezbollah took two Israeli soldiers hostage before retreating back to Lebanon. Israel called it "an act of war" and bombed Hezbollah positions in Southern Lebanon.

13/07/06: George W. Bush (President of the USA) defended Israel’s right to defend itself from attack while France, Russia and the EU were critical of a "disproportionate" use of force.

14/07/06: Hassan Nasrallah (the Hezbollah leader) called for "open war" against Israel.

15/07/06: Israel expanded it strikes on Lebanon striking Hezbollah strongholds and bombing central Beirut for the first time.

20/07/06: Israel continued to bomb Southern Lebanon by air while Hezbollah guerrillas persist in their rocket attacks into Israel.

14/08/06: A United Nations-brokered ceasefire went into effect.

Comment

In Lebanon, the Israelis faced terrain and enemy conditions for which they were not prepared. Israel tried to decide the issue with standoff air and artillery attacks but it did not stop the rocket attacks on Israel. Israel faced in Hezbollah neither an irregular opponent nor a state actor: a state sponsor (Iran in the case of Hezbollah) provided weapons and training to irregular forces. Hybrid organizations such as Hezbollah are well armed and equipped due to the availability of technologically advanced weapon systems at low prices and pre-existing commercial technologies such as cell phone and digital networks. During the Israel-Hezbollah War of 2006, decentralized cells (composed of guerrillas and regular troops armed with precision guided missiles, short and medium range rockets, armed unmanned aerial vehicles, and advanced improvised explosive devices) executed an irregular urban campaign against a conventional Israeli opponent. With Iranian Quads Force operatives as mentors and suppliers of advanced systems, Hezbollah cells downed Israeli helicopters, damaged Merkava IV tanks, communicated with encrypted cell phones, and monitored Israeli troops movements with night vision and thermal imaging devices. Hezbollah leveraged information technology as fighters immediately uploaded and distributed battlefield pictures and videos in near real-time, dominating the battle of perception throughout the operation.

The Israeli military did not lose the war in 2006 on the conventional battlefield, but did little to alter the strategic environment in Southern Lebanon and they lost the information campaign as the overwhelming perception within the international community was of Israeli military defeat at the hands of Hezbollah.
Estonia 2007

Root Cause: Russia disagreed on the relocation of the Bronze Soldier of Tallinn (Estonia removed the Bronze Soldier Soviet War memorial in Central Tallin).

27/04/07: Series of Cyberattacks, swampy websites of Estonian Parliament, banks, ministries, newspapers and broadcasters knowing that Estonia is the pioneer of E-government.

17/05/07: The Bronze Soldier riots erupted.

8-9/05/07: Second Wave of attacks on most celebrated dates in Russia.

17/05/07: 3-week wave of massive cyberattacks.

Comment

Estonia reported numerous incidents of Russian misinformation and destabilization campaigns against them. Estonia worked hard to back up all digital content relevant to state security and stability and normal functioning of the government in order to increase its resilience in the event of further cyber-attacks.

Estonians accused Russia of Waging cyber war by invoking Art. 5 of the Washington treaty. Even if a Cyber-attack is not a clear military action according to NATO, one cyber war can lead to much wider military conflict in such situations. Estonia was the first country claiming to be a victim of cyber war.

Georgia - Russia 2008

09/04/91: Georgia declared its independence.


01/08/08: Ossetia separatists began shelling Georgian Villages.

07/08/08: Georgia began a military operation in South Ossetia and took control of Tshinvali.

Russia accused them of aggression.

08/08/08: Russia launched a large-scale land, air and sea operation against Georgia with the stated aim of "Peace enforcement" + cyber-attack vs. Georgian Gov. website and information war.

12/08/08: Ceasefire negotiated by N. Sarkozy (French President):

– Some Georgian cities occupied,

– Some Georgian military less raided,

-- Ethnic cleansing of Georgians in South Ossetia.
26/08/08: Russia recognized Abkhazian and South Ossetia as separate republics. Georgia government severed diplomatic relations with Russia. 08/10/08: Russia withdrew its troops from Georgia:

– 192 000 people displaced,
– 20 270 people remain displaced as of 2014,
– Increase of Russian military presence in Abkhazia and South Ossetia in violation of the ceasefire agreement of August 2008.

Comment

It was difficult to prove the Russian’s state responsibility for cyber-attacks in Georgia but Report from the Georgian Foreign Ministry claimed that the Russian Business Network was actively engaged in cyberwarfare against Georgia.

At NATO conference in Wales, the organization extended the provision of Art. 5 of the Washington Treaty which regards an attack on one NATO country as an attack on all. NATO sent a clear message to Russia which supported or facilitated massive cyber-attacks on Estonia in 2007 and Georgia in 2008.

Syria - Islamic State since 2013

15/03/11: The unrest began in the early spring of 2011 within the context of the Arab Spring protests
08/11: Creation of Syrian National Council  15/07/12: The Syrian Free Army launched the Battle of Damascus
04/13: Hezbollah and Revolution’s watchman collaborate militarily with Damascus.
08/13: Chemical weapons against the Free Syrian Army
04/01/14: Battle between ISIS and Syrian’s rebel Militias
29/06/14: ISIS proclaimed Baghdadi, chief of ISIS, the new Caliph
09/14: The organisation proclaimed itself to be a worldwide caliphate and asked Muslims to swear allegiance to Baghdadi as a Caliph over Muslims.
2015: Many European and American people are believed to have joined IS in Syria.
08/15: Europe’s Refugees crisis (107,500 asylum seekers crossing EU borders in July).
09/15: Russia launched anti-ISIS op in Syria.
11/15: A Russian fighter was shot down in Syrian airspace by Turkey.
12/15: Russia unveils intelligence on Turkish-ISIS links
02/16: US-Russia deal on cessation of hostilities
03/16: Russia partially withdrew troops from Syria
Comment

Analysing the conflict in Syria through the filter of hybrid factors is by far too restrictive to completely understand the conflict: the two wars in Iraq, the permanent conflict between the two schools of the Arabic Islam and Bashar El Assad’s behaviour towards his people are obviously some significant key stakeholders of the conflict. What we analysed here is only one aspect of the conflict involving Europe: the use of internet and modern communication applications – not designed at all to support any military objective and coming from the West – in order to disseminate Islamic State propaganda and recruit soldiers for both the conventional war in Syria and terrorism in Europe.

Internet propaganda has been used as a mean to recruit some individuals from Western countries, in order to get them in Syria for training. To prevent any misunderstanding, we should immediately emphasize that Internet propaganda has nothing to do with Cyber warfare, a confusion made sometimes. It is only the way of leveraging the wonderful power of Internet (and applications such as YouTube, Facebook or Tweeter) for delivering its propaganda to large scale of people and then to make some in touch with individuals trained to finalizing the hiring and the trip to Syria.

Ukraine – Russia since 2014

12/13: Russian President Vladimir Putin agrees with Yanukovych on an economic lifeline, offering to buy Ukraine’s debt and reduce energy prices.

01/14: Clashes turn deadly when the government accepts new anti-protests laws. In late January, Ukraine Prime Minister, Mykola Azarov, resigned

02/14: Riots erupted in Kiev and a secession crisis began in Ukraine’s Crimean Peninsula. Pro-Russian gunmen seize key buildings in Crimea in late February.

07/04/14: Kiev launched a military operation in Ukraine’s east aimed at suppressing the growing independence movement among local citizens

03/14: Crimea voted to join Russia but the results have been internationally contested. The West dismissed the referendum as a sham and refused to recognize the vote.

13/04/14: The Ukrainian National Security and Defence Council decided to launch a full-blown operation with the use of armed forces to establish peace and order in Ukraine.

07/14: Malaysia Airlines flight is shot down over Eastern Ukraine. The west said the plane was shot down by pro-Russian insurgents.

11/14: 7 000 Russian troops inside Ukraine

02/15: Fighting continued regardless and Ukrainian forces pull back from the town of Debaltseva.

10/15: Russia had redeployed some of its elite units from Ukraine to Syria to support Syrian President Bashar-al-Assad.
Comment

Russia did not launch a traditional invasion to keep Crimea away from Kiev’s control. It has adopted a subtler approach intended to give the Kremlin “plausible deniability” while reducing costs associated with engaging Ukraine’s armed forces directly. The Kremlin is conducting a non-military, multi-vector hybrid war against Ukraine which is only visible to the West. In order to keep the Ukrainian state in a crisis mode, Russia is using different approaches: economic sanctions, cyber-attacks, international propaganda campaigns, militia groups (little green men) and political pressure which have many indirect consequences for the Ukrainian economy and society at large. In Ukraine, recent graduate are disillusioned, local entrepreneurs discouraged and foreign investors scared off. Russia wants to make Ukraine pointless which would remain dysfunctional in the face of continuing Russian threats, pressure and sabotage. Russia has been using an advanced form of hybrid warfare in Ukraine since early 2014 that relies heavily on an element of information warfare that the Russians call “reflexive control”.

Reflexive control causes a stronger adversary voluntarily to choose the actions most advantageous to Russian objectives by shaping the adversary’s perceptions of the situation decisively. Russian’s hybrid techniques in Ukraine

- Denial and deception operations to conceal or obfuscate the presence of Russian forces in Ukraine, including sending in “little green men” in uniforms without insignia,
- Concealing Moscow’s goals and objectives in the conflict, which shows fear in some and allows others to persuade themselves that the Kremlin’s aims are limited and ultimately acceptable,
- Retaining superficially plausible legality for Russia’s actions by denying Moscow’s involvement in the conflict, requiring the international community to recognize Russia as an interested power rather than a party to the conflict, and pointing to supposedly-equivalent Western actions such as the unilateral declaration of independence by Kosovo in the 1990s and the invasion of Iraq in 2003,
- Simultaneously threatening the West with military power in the form of overflights of NATO and non-NATO countries’ airspace, threats of using Russia’s nuclear weapons, and exaggerated claims of Russia’s military prowess and success,
- The deployment of a vast and complex global effort to shape the narrative about the Ukraine conflict through formal and social media.

Scenario References

1. "A closer look at Russia’s Hybrid War?" by Michael Kofman and Matthew Rojansky
2. "Military Capabilities for Hybrid War" by David E. Johnson
3. "Hybrid War: Old concept, New techniques" by Alex Deep for Small Wars Journal
4. "Is the EU’s failed relationship with Russia the member states’ fault?" by Anne Schmidt-Felzmann
6. "Core Software Security: Security at the source" by James Ransome and Anmol Misra
7. "Nothing New in Hybrid Warfare: The Estonian Experience and Recommendations for NATO" by Merle Maigre
8. "Russians may not be responsible for cyberattacks on Georgia" by Joel Hruska
9. "NATO’s Hybrid Flanks Handling Unconventional Warfare in the South and the East" by Andreas Jacobs and Guillaume Lasconjarias
10. "Putin’s information warfare in Ukraine" (Russia Report I) from the Institute for the study of war" by Marie Snegovaya
11. "Russian Hybrid warfare and extended deterrence in Eastern Europe" by Alexander Lanoszka
12. "Russian Hybrid warfare and other dark arts" by Michael Kofman
13. Russia’s pernicious Hybrid war against Ukraine” by Andreas Umland
Annex D: The System Dynamics Model and theory
System dynamics background

System Dynamics (SD) is a methodology related to both systems and chaos theory and has been used extensively to develop ideas and insights into the issues, problems, interdependencies and behaviours that are characteristic of dynamic complex systems. It was originally developed in the 1950’s and is widely used in both the public and private sectors for policy analysis and design [16].

How SD works – Causal Loop Diagrams and "feedback"

SD models are often presented in non-mathematical form as a Causal Loop Diagram (CLD) [17] which shows how each of the different variables are interrelated. Typically, variables are linked together with an arrow showing the direction of causation or flow of information or logic:

- A link marked positive (+) indicates a positive relation and a link marked negative (-) indicates a negative relation;
- A positive causal link means the two linked variables change in the same direction, i.e., if the variable in which the link starts decreases, the other variable also decreases. Similarly, if the variable in which the link starts increases, the other variable increases as well;
- A negative causal link means the two variables change in opposite directions, i.e., if the variable in which the link starts increases, the other variable decreases and vice versa;
- Links may be given a "+/-" dual sign indicating that the behaviour can be one or the other depending on interactions between the linked variables;
- Links may also be labelled with a 'D' indicating a time delay before an impact or outcome becomes apparent. Delays within a complex system can result in significant perturbations or fluctuations in one or more variables, making the system unstable.

An important aspect of the CLD is the identification and analysis of "closed cycles" which are either defined as a reinforcing or balancing loop. This feedback effect can drive significant behaviours within the system:

- A reinforcing loop is a cycle in which the effect of a variation in any variable propagates through the loop and returns to the variable reinforcing the direction of the initial change i.e., if a variable increases in a reinforcing loop the effect through the cycle will return an increase to the same variable. Likewise an initial decrease in a variable will propagate through the loop to force a decrease on this variable, leading to a ‘dampening’ effect;
- A balancing loop is the cycle in which the effect of a variation in any variable propagates through the loop and returns to the variable a deviation opposite to the initial one i.e. if a variable increases in a balancing loop the effect through the cycle will return a decrease to the same variable and vice versa; Reinforcing loops can lead to significant changes in how the system behaves in that the reinforcing...
effect of the variation will then create another reinforcing effect. Without breaking the loop the system is caught in a vicious cycle of circular chain reactions.

Working out feedback effects

To determine if a causal loop is reinforcing or balancing, one can start with an assumption, e.g. "variable 1 increases" and follow the loop around. The loop is:

- Reinforcing if, after going around the loop, one ends up with the same result as the initial assumption, i.e., reinforcing loops have either zero or an even number of negative links;
- Balancing if the result contradicts the initial assumption, i.e., balancing loops have an odd number of negative links.

Hybrid effectors

Box 1 shows a representative list of potential effectors that are available for use by any actor wishing to use such effectors. The term 'effector' has been chosen as a neutral term given that an effector can equally be used both offensively and defensively. The actual availability of an effector will be determined by the type, capability and world view of each actor, e.g., a Nation State, a terrorist cell or individual citizen will have very different degrees of access to some of these effectors and different views as to which ones they are willing or able to use. Some of these effectors have been ‘coded’ using ‘smiley’, ‘neutral’ or ‘unhappy’ faces simply to indicate the likely impact should the EU select one or more of these effectors.

Hybrid battlespace

Box 2 shows a representative list of the shared contested areas or ‘areas of influence’ ranging from the conventional ‘battlespace’, cyberspace and the key ‘human terrain’ comprising people as individuals and groups within an appropriate social, cultural, political, religious and economic framework that hybrid warfare attempts to influence and shape.

Hybrid CLD

The rest of the model shows each of the key variables and how they link and interact and provide causal impacts between hybrid effectors and the hybrid battlespace. The model is written to be agnostic of concepts such as ‘aggressor’ or ‘defender’; ‘small’ actors such as terrorist cells or ‘big’ actors such as Nation State or group of Nation States. The model does not assume two symmetrical or asymmetrical actors, thereby allowing for the possibility of multiple actors, each with differing levels of appetite, ability and capability to use hybrid effectors and all working within the same area(s) of influence. As such, the model should be considered to be at a very high level of abstraction, lacking detail and low level richness but still provides insights into how ‘hybrid warfare’ could be deployed and/or countered. Such detail can be generated but time constraints mean it is out of scope of SERA 28-Committee 2 paper (Informational and cyber warfare).
Hybrid CLD analysis

Resourcing Hybrid effectors

Box 2 feeds into Box 1 via “Areas of Influence”. This is an important variable as any actor will have to consider resource availability and prioritisation across a number of competing requirements and desired or acceptable outcomes. The link to this variable is given a “+” sign as this link will drive towards increasing or decreasing investment depending on the drivers within Box 2 and the influence of the other factors such as “Perception/National Interests” and “Decision making process”. It is worth noting that “Decision making process” has been given a ‘D’ marker indicating the potential complexities and time taken to reach a consensus decision between for example the EU 28 member states compared to a less democratic decision making process or a small group of activists or terrorists. Once resourced and prioritised there is a delay until these effectors are available to use shown by the delayed link from Box 1 to “Available hybrid effectors”. Again, this delay is important as the time take to field an advanced fighter aircraft or aircraft carrier can be measured in decades compared to a few hours to build and deliver an Improvised Explosive Device (IED) or the few minutes to set up and drive a social media account.

Using Hybrid effectors

Once available, hybrid effectors can be used in multiple ways as shown by the links to “Use of ‘blended hybrid effectors’” and “Use of countermeasures”. The term ‘blended’ is deliberate as the pool of “available hybrid effectors” can be viewed as an ‘a la carte’ menu from which an actor can choose the most appropriate mix of effectors and change this mix as the situation evolves. The use of both hybrid effectors and countermeasures are driven by a number of factors:

- **Effectiveness.** Effectiveness as shown by the positively signed links from “Effectiveness of hybrid effectors” to “Use of hybrid effectors” and the matching link from “Effectiveness of countermeasures” to “Use of countermeasures”. The negatively signed loops between “Effectiveness of hybrid effectors” and “Effectiveness of countermeasures” produces a reinforcing feedback loop essentially driving an ‘arms race’ as the actors seek to minimise the others’ effectiveness;

- **Political will.** Political will or acceptability of use as shown by the matching positive signed loops which take into account “Perception/National Interest” and “Decision making process” from Box 2 to both “Political will to use hybrid effectors” and “Political will to use countermeasures” and subsequently the matching positively signed arrows from the respective ‘political will to use…’ to the “Use of….” variables, recognising that willingness to use will drive actual use;

- **Strategic Outcomes.** The ‘heart’ of the model can be seen when considering the strategic outcomes. Both “Use of blended hybrid effectors” and “Use of countermeasures” are positively linked to “Likelihood of delivering favourable strategic outcomes” whilst also connected to “Likelihood of delivering unfavourable strategic outcomes” by negatively signed links: essentially, actors are attempting to use hybrid effectors
and/or countermeasures to reach favourable strategic outcomes whilst simultaneously reducing the likelihood of unfavourable outcomes. This logical link is shown by the variable “Favourable strategic balance”. It is connected to “Likelihood of delivering favourable strategic outcomes” by a positively signed link whereas the link from “likelihood of delivering unfavourable strategic outcomes” is negatively signed, illustrating that as the “Likelihood of reaching unfavourable strategic outcomes” increases, the “Favourable strategic balance” begins to favour other actors resulting in either a switch in hybrid tactics and a different mix of effectors and/or countermeasures or a reduction in the use of hybrid tactics and countermeasures;

- **Strategic Outcomes and Perception.** “Favourable strategic balance” is connect to Box 2 via a delayed link called “Awareness”. This is an important link as the actors do not have perfect information and the quality and quantity of intelligence, information and effectiveness of decision making will take time to become evident. Again the actors will be operating with different world views, decision making cycles and time frames. Perception plays a large part in strategic outcomes as shown by the matching delayed links from Box 2 to “Perceived ‘acceptable’ Low Threshold (Opponent’s red lines firm), (Friends/Allies/Own Population broadly unsupportive)” and “Perceived ‘acceptable’ High Threshold (Opponent’s red lines not firm), (Friends/Allies/Own Population broadly supportive)”. The first variable represents an unfavourable environment for the actors and one more likely to tilt “Favourable strategic balance” against them. In comparison, Perceived ‘acceptable’ High Threshold (Opponent’s red lines not firm), (Friends/Allies/Own Population broadly supportive)” provides a more friendly environment for the actors in which “Favourable strategic balance” favours their strategic outcomes;

- **Reinforcing Loops.** The bulk of the feedback loops in the model are reinforcing loops which drive the behaviour of the model to either invest in hybrid effectors and countermeasures, deploy these until such times as “Favourable Strategic balance” begins to favour other actors;

- **Balancing Loops.** There are 2 balancing loops each driven by the links from Box 2 to “Likelihood of delivering unfavourable strategic outcomes”. The first loop runs from Box 2 via a delayed link to “Perceived ‘acceptable’ Low Threshold (Opponent’s red lines firm), (Friends/Allies/Own Population broadly unsupportive)” to “Likelihood of delivering unfavourable strategic outcomes” and “Favourable strategic balance” then back in Box 2. Essentially the actors are now in an unfavourable environment in which the strategic balance no longer favours their tactics or approaches. However, this loop initiates a longer loop with unexpected consequences. As the “Likelihood of delivering unfavourable strategic outcomes” increases it reduces “Political will to use hybrid effectors” which in turn reduces the “Use of hybrid effectors”. As “Use of hybrid effectors” decreases the ““Likelihood of delivering unfavourable strategic outcomes” increases again resulting in unfavourable strategic balance. At first glance this appears counter-intuitive as hybrid effectors are meant to reduce the probability of triggering unfavourable responses, in this case the other actors’ awareness and unfavourable support now forces the actors to change tactics or to come to an accommodation.
## Annex E: Hybrid Risk Assessment Methodology Results

<table>
<thead>
<tr>
<th>Hybrid Factors</th>
<th>Hybrid Effector</th>
<th>Outcome / Reasoning</th>
<th>EU</th>
<th>Other Nations</th>
<th>Terrorists</th>
<th>Impact on other Nations</th>
<th>EU against other Nations weakness --&gt; strength</th>
<th>Impact on Terrorism</th>
<th>EU against terrorist organisations weakness --&gt; strength</th>
</tr>
</thead>
<tbody>
<tr>
<td>Military Unconventional</td>
<td>WMD (Chemical &amp; Biological only)</td>
<td>Unacceptable under 1992 CWC and 1972 BTWC</td>
<td>--</td>
<td>-+</td>
<td>++</td>
<td>n/a</td>
<td>0</td>
<td>n/a</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>Nuclear Deterrent Capabilities</td>
<td>Provide Nuclear Deterrence</td>
<td>-</td>
<td>-+</td>
<td>--</td>
<td>n/a</td>
<td>0</td>
<td>n/a</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>Special Forces</td>
<td>Provide special operations</td>
<td>++</td>
<td>++</td>
<td>--</td>
<td>+</td>
<td>3</td>
<td>++</td>
<td>4</td>
</tr>
<tr>
<td></td>
<td>Militias</td>
<td>Provoke disorders</td>
<td>--</td>
<td>-+</td>
<td>++</td>
<td>n/a</td>
<td>0</td>
<td>n/a</td>
<td>0</td>
</tr>
<tr>
<td>Military Conventional</td>
<td>Land Capabilities</td>
<td>Project Forces (land military operation)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>----------------------</td>
<td>-------------------</td>
<td>------------------------------------------</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Defend the Nation</td>
<td>++</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>++</td>
<td>++</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>--</td>
<td>++</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>--</td>
<td>--</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>++</td>
<td>--</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>++</td>
<td>-1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>++</td>
<td>++</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>++</td>
<td>-2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Air Capabilities</td>
<td>Support Allies</td>
<td>++</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>++</td>
<td>++</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>--</td>
<td>++</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>++</td>
<td>3</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>++</td>
<td>++</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>+</td>
<td>--</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>+</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>+</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Maritime Capabilities</td>
<td>Support International Operations</td>
<td>++</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>++</td>
<td>++</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>--</td>
<td>++</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>+</td>
<td>3</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>++</td>
<td>3</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>+</td>
<td>3</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Space Capabilities</td>
<td>Enforce International Operations</td>
<td>++</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>++</td>
<td>++</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>--</td>
<td>++</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>+</td>
<td>3</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>++</td>
<td>3</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>+</td>
<td>3</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cyber Capabilities</td>
<td>Support International Treaties (BI and Multi-lateral)</td>
<td>++</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>++</td>
<td>++</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>--</td>
<td>++</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>+</td>
<td>3</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>++</td>
<td>3</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>+</td>
<td>3</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Economics</td>
<td>Basic food/water</td>
<td>Deny access to basic food/water</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>--</td>
<td>--</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>--</td>
<td>++</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>++</td>
<td>+</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>++</td>
<td>-1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>++</td>
<td>+</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>--</td>
<td>-2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>++</td>
<td>--</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>++</td>
<td>++</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>++</td>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>+</td>
<td>+</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>+</td>
<td>3</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Energy</td>
<td>Deny access to Energy supplies</td>
<td>+</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>+</td>
<td>--</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>+</td>
<td>++</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>++</td>
<td>+</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>++</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>++</td>
<td>++</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>++</td>
<td>2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Internet</td>
<td>Provide dis-information/propaganda</td>
<td>--</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>--</td>
<td>++</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>++</td>
<td>++</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>+</td>
<td>--</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>++</td>
<td>--</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>++</td>
<td>+</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>+</td>
<td>-2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>+</td>
<td>-</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>+</td>
<td>-1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Law</td>
<td>Support International Institutions/Trade Agreements</td>
<td>++</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>++</td>
<td>++</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>--</td>
<td>++</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>++</td>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>++</td>
<td>+</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>+</td>
<td>3</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Commerce</td>
<td>Access to internal and international markets</td>
<td>++</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>++</td>
<td>--</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>--</td>
<td>++</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>++</td>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>++</td>
<td>+</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>+</td>
<td>3</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Political /Diplomatic</td>
<td>Gunboat Diplomacy</td>
<td>Support National Policies</td>
<td>++</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>++</td>
<td>++</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>--</td>
<td>++</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>+</td>
<td>3</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>++</td>
<td>++</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>+</td>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>++</td>
<td>++</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>++</td>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>--</td>
<td>++</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>++</td>
<td>3</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Intelligence</td>
<td>Support National Industries</td>
<td>++</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>++</td>
<td>++</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>--</td>
<td>++</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>++</td>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>++</td>
<td>+</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>++</td>
<td>3</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Law</td>
<td>Support Allies</td>
<td>++</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>++</td>
<td>++</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>--</td>
<td>++</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>++</td>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>++</td>
<td>+</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>++</td>
<td>3</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>++</td>
<td>++</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>++</td>
<td>3</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Society</td>
<td>National 'norms'</td>
<td>Provide own viewpoint and counter information</td>
<td>++</td>
<td>+</td>
<td>--</td>
<td>-</td>
<td>1</td>
<td>+</td>
<td>3</td>
</tr>
<tr>
<td>------------------</td>
<td>------------------</td>
<td>-----------------------------------------------</td>
<td>----</td>
<td>---</td>
<td>----</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>Free Media</td>
<td>++</td>
<td>-</td>
<td>++</td>
<td>+</td>
<td></td>
<td></td>
<td>3</td>
<td>-</td>
<td>1</td>
</tr>
<tr>
<td>Social Media</td>
<td>++</td>
<td>++</td>
<td>++</td>
<td>+</td>
<td></td>
<td></td>
<td>3</td>
<td>-</td>
<td>1</td>
</tr>
<tr>
<td>Internet</td>
<td>++</td>
<td>++</td>
<td>++</td>
<td>+</td>
<td></td>
<td></td>
<td>4</td>
<td>+</td>
<td>3</td>
</tr>
</tbody>
</table>
Committee 3

How can the EU/Europe/European industry support maintaining and/or reshaping EDTIB for an age of the hybrid warfare?

Pilot: Doris LAARMAN, Jan ENGMANN, Wim TJSTERMAN

Members of the Committee

Michael MEW (Chairman)
Karina GLAPKA (Secretary)
Reinhard MARAK
Anu ESLAS
Tommi NORDBERG
Hervé MANIÈRE
Frode Narum HANSEN
Nils WALLHED
Igor DOBROVIC
Rob ZUIDDAM
Nicolas TALLAT
Hybrid warfare extends the scope of conventional military operations – adding a wider spectrum of threats and blurring the boundaries of classical defence, security and civilian industries. It exploits new technologies (cyber, media, communications, etc.) in particular those developed in the civilian domain – as well as classical military systems.

As such it places both an opportunity and a challenge on the EDTIB.

The integrated European concept of an EDTIB has not significantly progressed. It is mainly a "collection" of national DTIBs – with varying levels of international integration, "over capacity" and duplications. Cooperation across Europe.

The primary challenge of the "hybrid" era on EDTIB will be to provide more capabilities within broadly static (even decreasing) defence budgets. "Classical" capabilities such as aircraft carriers, submarines, etc. – with long lifecycles, and little/no civilian application will still be required, but in addition new solutions will need to be provided. These must be quickly introduced to respond to emerging asymmetric or hybrid threats – and may be adapted from technologies with primarily civilian applications.

In light of this, the EDTIB needs to focus on two axes:

**Delivering Existing capabilities more effectively** Increased Collaboration across European players to deliver "classical’ defence capabilities more cost-effectively, reducing duplication in R&D, Development and in-service systems – maximising the outputs of European Spend

**Delivering new and innovative capabilities quickly.** A more active approach to identifying & exploiting Civilian technologies – to understand how to counter the threats they pose when in the hands of adversaries, and to integrate them into European defence systems to provide advantage. The role of the EDTIB must be to focus on “niche’ capabilities required to exploit and make these capabilities robust for military use rather than for

There are many actors within the EDTIB and they each need to play their part. Recommendations for EU, nation states, European agencies and industry are provided.

**Introduction**

The security environment in the EU is unstable, complex and fragile. The most topical security threats of today are related to hybrid operations driven or at least influenced by State parties on one hand and international terrorism on the other.

In view of this, security and defence need to have a central place on the European agenda. The main challenge is to make full use of all available military capabilities and tools, including the European Defence Technological and Industrial Base (EDTIB), to achieve the aims of the EU Common Security and Defence Policy (CSDP).
In this endeavour, a number of different actors, such as European States, institutions and other entities play their distinctive roles. In this respect European industry forming the EDTIB is also a key element in the European security architecture.

The question still is: is the EDTIB fit for today’s and future challenges?

**Hybrid warfare – Understanding rather than defining**

The hybrid warfare concept re-emerged in 2014 with the developments to the east to the European Union. Especially media and politicians have been using this term frequently to describe complex and multi-layered operations driven or at least strongly influenced by state parties, not reaching the level of a conventional state-to-state conflict. The impression thus arises that this is a new and highly effective form of warfare confronting the European states, the EU and NATO with complex challenges.

Hybrid warfare is not defined – in other words, the engaging individuals (the equivalent of combatants in a conventional conflict) are acting in a legally not fully defined situation, again raising questions on the lawfulness of respective countermeasures.

Various preliminary stages in the concept were discussed in the early 2000s using terms such as "4th generation warfare" and "compound warfare". The term "hybrid warfare" was first used in 2005 by the US military author and political scientist Frank G. Hoffman. It became more widespread after the 2006 war in Lebanon. Hoffman defined hybrid warfare as a generally simultaneous and synergistic combination of conventional and irregular warfare in conjunction with acts of terrorism and criminal behaviour in a war zone, in order to achieve political objectives.

The term was intended to denote an allegedly new type of complex warfare and a range of multi-dimensional threats to which there could be no appropriate military response. However, the term hybrid warfare is often used glibly and a wide range of attributes are ascribed to it. It should also be noted that warfare has always been characterised by complexity, momentum, risk and lack of transparency, and that it develops in an environment of conflicting rational, emotional and random conditions. Without placing it in the relevant context, the term hybrid warfare is therefore unsuitable for use as an analytical tool. It appears to make more sense to describe the type of warfare on a case-by-case basis rather than attempting a definitive definition.
Hybrid warfare and Technology

Though hybrid warfare cannot easily be defined, one common denominator is the enlarge use of civilian technology.

A few years ago defence industry was virtually driving the technological development, but this has dramatically changed in recent years. The innovation centre has shifted from defence to the civil sector. This paradigm shift, combined with the fact that defence research and development budgets have significantly declined, makes it ever more important leveraging civil investments and ensuring that defence investments is targeted in areas where it can add the most value and not duplicate existing investments.

As examples, the massive drive within the civilian internet, social networks, cloud services, gaming industry, Internet of Things (IoT) and mobile industry, where billions of consumers push the innovation forward, need to be utilized by the defence forces while still maintaining their special needs for security.

A constantly increasing technological development worldwide leads to a growing number of primarily civil-related technologies that should be exploited by defence forces. Civil-driven innovation can possibly be game-changing for the defence forces, whereas defence developments traditionally only results in linear progress. Adapting and integrating civilian-led developments is critical for the defence forces demand to maintain cutting-edge technologies without bearing the full burden of costs. This should give great possibility to develop better and more cost effective military solution, but the defence forces seem to struggles to adapt new technology to military requirement, often resulting in an unwanted gap between the two user groups. A gap an asymmetric adversary can utilize.

But this civil innovation should not take place in isolation, but rather benefit from interactions from a range of actors. For certain potential technological areas defence focused actors, such as defence research agencies and/or defence industry, should therefore seek involvement to ensure the best possible outcome for the defence forces. Artificial intelligence leading to self-operated, fully autonomous systems, social network and cloud services concepts applied to Network Based Defence or the utilization of nanotechnology are just some examples where defence focused actors could contribute ensuring usability in future defence solutions.

(1) http://www.rand.org/content/dam/rand/pubs/research_reports/RR400/RR478/RAND_RR478.pdf - Future Technology Landscapes - Insights, analysis and implications for defence
**Actors and Stakeholders**

The multi-layer security architecture we can presently see in Europe has a number of players who all have a certain degree of bearing on the overall security and defence situation. These actors can be divided in basically two main groups: governmental and non-governmental bodies.

The primary governmental bodies are States, who, particularly in the defence and security area still are the main drivers. Another group of important security and defence actors are more or less formal, different sized groups of States. Particularly interesting in the security and defence world are the LOI-6 group, the Nordic Defence Cooperation (NORDEFCO) the Visegrad Group or the UK-French defence cooperation.

In addition, we have a multilayer system of international organisations and institutions, such as the European Union with its various bodies, OCCAR, NATO, the OSCE and the UN. All of those institutions have a security – and in many cases – a defence dimension.

Apart from governmental bodies, we also face a number of non-governmental actors. There is a substantial number of enterprises and academic players that form the EDTIB. Many enterprises group in national and international associations like the AeroSpace and Defence Industries Association of Europe (ASD).

On top of this, we can see a growing number of Non-Government-Organisations (NGOs), such as Amnesty International, Human Rights Watch or Transparency International, which increasingly engage in the broader security and defence area. Last but not least, in modern societies also traditional and social media play a decisive role and has a substantive impact on public opinion.

A closer look at each of these players and their respective roles in comparison with hybrid threats is undoubtedly beneficial.

**States**

States are the primary subject of international law and the bearer of sovereignty. It is a State’s principle responsibility to ensure inner and outer security for its population. In modern international law we dedicate to the State a monopoly of using force to ensure this inner and outer security. As hybrid threats have an impact on both the inner and outer dimension of security, the single state has the responsibility to address these hybrid threats with an adequate response. In a traditional concept, it was less complicated to make a distinction between inner and outer threats and hence to address them with the respective bodies, police for the internal security, the military for the external security. As hybrid threats by nature combine both, it becomes less and less possible to make a clear distinction, requiring a closer cooperation between the different actors.

It goes without saying that with the increasing blurriness of the dividing line between inner and outer security and the growing number of new threats, the tools to address these threats need
to become more comprehensive and also the governmental bodies using them will become more numerous. States will also have to address the legal basis for countering these threats. As the restrictions of internal security measures are primarily set by human rights, an armed conflict is predominantly governed by international humanitarian law, allowing the State to use a totally different amount of force to implement its interests.

As hybrid threats comprise, besides a more or less conventional application of violence, a number of "softer" ways of force, the States will have to be respectively creative in developing appropriate countermeasures. Making public opinion more resistant against foreign "psychological" measures, such as propaganda or infiltrating fears and instability, will probably be as important as developing technical capabilities.

In the Security and Defence area States and particularly European Member States tend to form groups to identify and consequently pursue common interest. Prominent clusters of the defence world are the LOI-6 group and OCCAR. The LOI community, summoning the biggest defence materiel producing countries in Europe, namely France, Germany, Italy, Spain, Sweden and the United Kingdom, with more than 90% of the overall defence industrial turnover in Europe plays a vital role in European defence industrial and technological development, particularly as the group has dedicated sub-groups on research & development and security of supply.

OCCAR, the Organisation for Joint Armaments Cooperation, founded by Belgium, France, Germany, Italy, Spain and the United Kingdom and open to other countries for project-specific armaments cooperation, focuses on the common development of systems and thereby could also play a more prominent role in countering hybrid threats in the future.

Besides these most known European players, NORDEFCO and the Visegrad group play a role in defence cooperation. Both represent a more or less intensive cooperation between groups of European States. Other examples of cooperation forums include the UK-French defence cooperation or the DACH initiative in which Germany, Austria and Switzerland discuss topics of defence cooperation.

But also in the field of police cooperation we see the formation of clusters such as the Forum Salzburg, a loose cooperation between central and eastern European Ministers of interior, striving for more multilateral collaboration, particularly in the cyber area. Lately, the Forum Salzburg was used as a platform to identify possible ways to manage the migration situation on the eastern borders of the European Union.
International Organisations

A vital role in the maintenance of security in Europe has to be assigned to the European Union with its institutions, the Council, the European Commission and the European parliament and their respective sub-bodies.

A central part here is certainly been given to the European Council, the collegial body of the Heads of States and Governments who gives the basic strategy guidance to the European Union. The Council Conclusions of December 2013 and June 2015 addressed the security and defence sector intensively and paved the way for the current action in the Council working bodies and the European Commission. The European Council is also the perfect place to bridge the blurring dividing line between the security and defence world.

The European Commission lately pushes further into the defence domain which was for a long time considered to be out of its scope. Only lately, particularly through its competences in industrial and market policy, the Commission entered the defence field, most recently – and perhaps most important in respect of hybrid warfare – through its efforts to set up a research and technology programme on CSDP to complement the European Union’s security research. Applied in a coherent way, both programmes have the potential to shape the European industrial base to fit the future security challenges.

A specifically relevant EU-player is the European Defence Agency (EDA). EDA, which has been created to support defence cooperation over the entire spectrum — capability development, R&T collaboration, armaments cooperation and common defence industrial policy — is currently is more focused on initiating the cooperation in specific areas of interest for the member states, supporting it through developing incentives for cooperation (e.g. VAT exemption, common procurement) as well as coordinating with other EU institutions in ensuring the defence dimension in wider EU policies (e.g. use of the European Structural and Investment Funds, or COSME® financial instruments for defence). Four ongoing strategic projects of EDA relate to air-to-air refuelling, Remotely Piloted Aircraft Systems (RPAS), government satellite communication and cyber defence.

Another important organisation in this respect is the North Atlantic Treaty Organisation (NATO), which, starting from the concept of collective self-defence, has over the years built a robust organisational structure to address all sorts of defence cooperation. Though NATO engages also in industrial topics, particularly through the NATO Industrial Advisory Group (NIAG), its powers and funds are still limited when it comes to industrial policy.

The OSCE has a particular role in the wider European dimension. Over quite some years it has been regarded as more or less dormant but has lately started to become a central hub for addressing hybrid situations again. Particularly in the crisis regarding Crimea and Donbas, the OSCE could again serve as a forum to monitor hybrid conflict.

(© EU programme for the Competitiveness of Enterprises and Small and Medium-sized Enterprises, running from 2014 to 2020.)
Last but not least the United Nations’ (UN) part has to be mentioned. Though the UN is, in principle, the primary actor in maintaining peace and stability worldwide, it has difficulties to address situations that are below the threshold of conventional conflicts. Even more so that their main body, the Security Council, is increasingly often blocked due to the different opinions of the veto powers. Nevertheless, there is a significant number of countries worldwide who would only engage in an international operation to address a hybrid threat if there is a mandate by the UN Security Council.

Industry

Also industry plays a vital role in developing an industrial base to counter future hybrid threats. However, industry needs a clear picture of the demand of its customers to be able to develop the right technological skills. Particularly in a market that is as unique as the security and defence sector, industry needs certainty and predictability, as well as financial support for investments the return of which cannot be foreseen.

The defence and security market is characterised by a rather small amount of customers – basically states – and a respectively small number of suppliers. The products both for conventional and hybrid warfare are all to be at the very high technological end, which again requires industrial leaders to take high risk decisions on their investment, particularly when it comes to invest into new technologies to counter new threats.

Other players

Particularly in hybrid situations, NGOs and traditional and social media play a vital role in influencing the public opinion, especially as either side of a hybrid conflict will try to use this influencing power for their own advantage. Whereas state-driven propaganda should definitely be a concept of the past, a closer cooperation with these non-state actors could still be beneficial. An open and transparent way of communication, also addressing their responsibility could eventually lead to their support in countering hybrid threats.
10 years of EDTIB

Defence industry in Europe is well placed technologically and organisationally to develop, manufacture and operate virtually all military systems and installations to high quality standards. It is a highly innovative sector, with important spin-offs in other areas such as electronics, space, and civil aviation.

However, defence is also a very specific sector, where the relation between the demand and supply side is stronger, more symbiotic and difficult. There is a heavy government influence on the sector, and this strong – in terms of capabilities – defence industry contrasts with weaknesses in terms of defence policy.

For many years, defence business was predominantly national. Only in last 15 years the declining defence budgets forced the governments to cut back the spending, to look for cooperation and industry – to look for other markets.

With limited demand and first shy attempts at cooperation, defence sector started to be assessed in its European aspect. At the government level, fragmentation of demand became obvious, with separate planning cycles, requirements and procurement procedures. This governments’ lack of decidedness, combined with procurements from national industries, on the supply side resulted in duplication of industrial capabilities – there are three 4/4+ generation fighter jets built in Europe, six submarines programmes in place and about 20 programmes of armoured vehicles.

With reducing budgets and shrinking defence forces, focus is put on multinational cooperation. Increased development cost combined with fewer units often result in very high unit prices, again putting focus on international cooperation, though this has not proven to be as easy and effective as desired. At the same time technological development speed is increasing and system complexity is growing. Considerable changes in defence industry over the last years have resulted in the number of different suppliers reducing. Defence forces are therefore becoming increasingly dependent on a consolidated industrial base for support and maintaining knowledge of the complex systems.

The concept of the European Defence Technological and Industrial Base (EDTIB), as we know it today, was introduced in 2007, when EU defence ministers called for capability-driven, competent and competitive defence industry in Europe. The ministers did not define what an EDTIB is (till this day, it is mostly understood as a sum of national defence industries), and focused only on the desired outcome – better coordinated, less duplicative defence landscape, able to ensure the right military capabilities for Europe(3).

A number of initiatives spun off the EDTIB Strategy, including an attempt to identify and address key industrial capabilities in different industry sectors, developing the support for small and medium-sized enterprises (SMEs) and undertaking joint efforts for security of supply (SoS). The Strategy also highlighted the need for more cooperation in armaments, increased investment in research and consolidation of demand.

However, the impact of the Strategy and the follow-up actions has been limited and focused mostly on soft, political measures and recommendations, not binding for the governments – e.g. for SMEs or SoS. In the market area, the European Commission soon took over the lead with its "defence package" (directives 2009/81 on defence and security procurement and 2008/43 on intra-Community transfers and their communication "Towards a more competitive and efficient defence and security sector"), introducing regulatory measures in procurement and transfers of armaments. Both Directives are currently under review in terms of their implementation, use and impact on the defence market. The key questions relate to their effect on increasing cross-border contracts, particularly for SMEs.

Within EDA, a number of joint projects have been launched, but predominantly in the research area, rather than armaments development – out of the numerous R&T projects, only 2 have moved to OCCAR for further development (ESSOR, MUSIS).

The importance of EDTIB was reiterated on numerous occasions at the political level – by the European Council, by the European Parliament, EU defence ministers.

But in the end, the landscape of the EDTIB has not changed significantly over the last years. One of the reasons is definitely a significant decrease in defence spending - but, instead of being a driver for cooperation, it seems to be an argument for the governments to buy armaments nationally – thus investing in their own economy. Cooperation can propose the solutions to the problems, but at the same time the commitment to change is limited.

Where there is cooperation in the area of defence, it is still mostly intergovernmental. This form of collaboration has the strongest influence on the structure of EDTIB. For example, Germany and France have been working together since the 1950s on the manufacture of the Transall transport aircraft. Typical features of such cooperation are that it is ad hoc and the EU plays no role in it. In addition, it virtually only comes into effect when the countries are unable to undertake a defence project alone (lack of funding or know-how). Otherwise, states prefer to use their own products and manufacturers.

Cooperation however does not necessarily mean better value for money through competitive processes. In cooperative projects, states typically organise the procurement of defence equipment among themselves using the rules of proportional allocation. In multinational defence projects such as the Eurofighter, orders are split and allocated among companies in the participating countries. The split is proportional to the country’s financial share of the overall project (juste retour). In OCCAR, the member countries agreed to apply a principle of global balance instead – the work share is balanced over a number of programmes and years.
Moreover, the EU states, particularly in the current security situation, often use the argument of essential national security interests. This is an exception from EU procurement rules on the basis of the article 346 of the Treaty on the Functioning of the European Union (TFEU). Here, the competition or competitiveness are not the main arguments – it is largely security of supply in view of future threats. This choice between effectiveness in acquisition of armaments and safeguarding national security needs is a difficult one to balance.

Not only was the progress towards EDTIB quite slow, the governments also contradict their own objectives when industry tries to make an effort – for example, when BAE Systems and EADS (now Airbus) announced their plan for a merger in 2012, it was the governments that blocked the deal through their shares in the companies. The main reason for this failure was a lack of agreement over the proposed solutions related to the governments’ control over the company.

However, one can also observe a tendency of industry to happily accept a domestic preference when it comes to their own home market on one hand, whereas, on the other hand, they complain fiercely against the same approach when applied in another market.

When in June 2013 the European Parliament issued a report on the status of the formation of the EDTIB outlined in 2007, it stated that the joint political vision has lost contact with the individual political and industrial reality of the growing export orientation of European countries and its suppliers. The EDTIB is summarised to be trapped between the national interest and the global developments.

**Impact of hybrid warfare on EDTIB**

Increasingly blurring lines between typical military and civilian threats, needs and capabilities are one of the key challenges in addressing hybrid warfare.

Countering hybrid threats still requires the use of conventional defence equipment. The requirements and main characteristics of such equipment are still valid. It will continue to be developed in a longer, 30 to 40 years’ life-cycle. Defence systems, as developed for customised, specific requirements, will (as they already are) be expensive, mainly State funded and will hardly have any potential dual-use on the civilian, commercial market. There is however a room for improvement – more efficiency and focus on progress and not on national specificities is needed.

There is a growing need for including and exploiting civilian technologies and solutions within the process. In many areas, for example communication networks, civilian capabilities are now more advanced than the ones exclusively developed for the military purpose. These technologies, characterised by their short life-cycle and an obsolescence of about 2 to 3 years, are

---

often easily available of the shelf for everybody, whilst the conventional defence forces wait for their customised solutions.

Currently, there is no industry that can be categorised as "hybrid industry". Taking into account that addressing hybrid threats would require a mix of capabilities, the current EDTIB should be ready to include non-traditional defence suppliers. More flexibility, agility and innovation would be required from industry in response to hybrid threats, not only in terms of technology, but also in cooperation and new business models. The question still remains whether the then expected State influence in these domains would lead to the same market distortions as for the "conventional" EDTIB.

When it comes to public procurement of capabilities to counter hybrid threats, the current rules for defence and security acquisition might lack flexibility, as they tend to be lengthy and complex. In the process of reshaping the EDTIB, addressing the legal framework is vital. For the development of capabilities needed to counter hybrid threats we need a legal environment that allows all the players involved to do their part as effective as possible.

Whilst hybrid warfare requires the maintenance or enhancement of traditional capabilities, as well as the addition of new capabilities, such as cyber, etc., it implies that budgets need to spread even further. Moreover, the fact that hybrid warfare presents "supra-national" regional threats that affect European nations at a collective level should mean that common capability requirements emerge and more cooperation should be expected. However, the hybrid threat could also present a significant threat to collaboration – and to the EDTIB itself – as nations might tend to resort to "off-the-shelf" purchases in response to capability needs that are emergent and urgent.

The different issues arising from hybrid threats are being recently widely discussed, and the industrial involvement is one of the aspects addressed.

One prominent document addressing hybrid threats is the European Commission’s report on countering hybrid threats at the European Union which identified a number of actions with a possible impact on the EDTIB:

- Creation of an EU Hybrid Fusion Cell, capable of receiving and analysing classified and open source information on hybrid threats.

The tools and services to be able to operate the fusion cell will be provided via the existing industry base as well as new entities. This will lead to a transformation of the EDTIB where new entities will be integrated with traditional defence and security industries. Therefore mechanisms must be implemented there the traditional industries are collaborating with new entities in the arena. The structured, process driven and more slowly moving industries need

---

to effectively interact with smaller, agile but technically sophisticated companies to be able to create appropriate solutions.

✓ Establishing a Centre of Excellence for "countering hybrid threats".

The centre is proposed to focus on researching how hybrid strategies have been applied, and encourage the development of new concepts and technologies within the private sector and industry to help Member States build resilience. The centre should design programs to advance research and exercises to find practical solutions to existing challenges posed by hybrid threats.

The programs launched in the centre are foreseen to address the existing industry base as well as new entities in the research area. This will lead to a transformation of the EDTIB where new entities again will be integrated with traditional defence and security industries.

✓ Preparation for the next generation of GovSatCom at European level and the introduction of Galileo in critical infrastructures dependent on time synchronization.

Effectively sharing information, close to real-time, is one of the key success factors on countering the hybrid threats. Having mechanisms for enabling information superiority are essential. The time stamp and sharing the same understanding of time is critical to be able to build up that level of information. Therefore the new entities on the arena need to integrate functions of Galileo in their systems. The new entities must be able to integrate existing legacy solutions in the new systems.

✓ The Commission, in coordination with Member States, will work together with industry within the context of a contractual Public Private Partnership for cyber security, to develop and test technologies to better protect users and infrastructures against cyber aspects of hybrid threats.

The proposed PPP for cyber security will have a direct impact on the existing and additional new EDTIB. The PPP needs, in addition to facilitate and integrate the different parts of the extended EDTIB, to address the importance of a much faster procurement process. Governmental procurement processes applied by the member states often lead too long time to market. Systems are relatively old when the reach the end user. The PPP needs to be able to directly buy from vendors on occasions in order to quick response on new unforeseen threats.
Recommendations and Summary

The EDTIB, as we know it, has to cope with the new threats of the hybrid age and to deliver additional outputs:

✓ Delivering existing capabilities more efficiently
To address new capability shortfalls deriving from hybrid threats, traditional capabilities would need to be delivered more efficiently and at a lower price. The remaining funds could then be invested into the development of measures to counter new challenges or adapt existing solutions to the needs of the customer. Likewise would the EDTIB need to evolve respectively.

✓ Delivering new capabilities quicker
In an increasingly faster changing threat environment, the EDTIB needs to find ways to identify mature integrate and deployed technologies in much shorter time scales than in traditional programmes. This would for example require new approaches to certification, specifically through less bespoke trials or acceptance procedures, making evidence available and acknowledged by multiple nations.

✓ Adapting and evolving
Product life cycles that allow incremental updates and spiral developments enabled by open architectures and a more modular approach need to be embraced, such as the example of the Gripen flight control software development.

✓ Innovation
An EDTIB of the future would need to be even more innovative to counter the evolving hybrid threats. Innovation across the entire spectrum of hybrid warfare would need to be encouraged by investing more in research and developments but also in improving the processes and methods for exploiting the outputs at the European level. The Preparatory Action on CSDP-related research is a perfect example of how this could work in a European context.

All of those topics would need a respective involvement of all relevant actors.

States

It goes without saying that sufficient defence spending is essential for the EDTIB to remain competitive and able to deliver to the needs of the customer. As already pointed at the European Council in Hampton Court in 2005 we need to "spend more, spend better and spend more together". In essence, it is still the States who define their overall, and hence defence, budget. A more holistic approach between security and defence spending might also bear potential for synergies and thus for savings.

Industry needs to be involved at an early stage to ensure that they can adapt their solutions to the upcoming requirements of the user. A clear picture of future threats by industry would reduce the risk of failed investments.
It is up to the States to drive cooperation.

The Hybrid threat creates an opportunity, and an imperative, for better cooperation/coordination between States in areas of interest. Communities of states need to improve their threat assessment & sharing of intel. info, lessons learned, and capability assessment (identification of potential solutions).

States need to actively seek deeper cooperation on classical defence systems (in order to achieve better value for money) whilst also collaborating in new and emerging and emerging areas of interest. Overcoming the traditional "national security’ concerns of pooling/sharing in emerging areas of defence and security is a key enabler for this. States should also better support organisations established to enable cooperation, and use of existing tools (e.g. CODABA).

Another key role for nation states is in the encouragement / enforcement of industrial restructuring in order to deliver a more effective and streamlined EDTIB. Too often the states act as "regulator’ in national procurements, protecting national jobs, industry on a short-term basis. A longer-term, broader view is required, looking to establish a balanced workshare over multiple contracts – and accepting a level of dependency on capabilities within other nation states.

**European organisations and institutions**

There are many ongoing initiatives at the European level that have an impact on EDTIB, such as the EU Global Strategy, the European Commission’s Report on countering hybrid threats (published in April 16) or the upcoming European Defence Action Plan.

However, the main task would be to ensure that these different actions and recommendations are followed through, with funding and proper implementation.

Some areas of known weaknesses have already been identified which must be improved:

- more R&T collaboration is needed,
- implementation and application of EU legal framework, particularly the ICT & procurement directives
- financing initiatives should be improved to enable cooperation and export.

Finally, perhaps the various initiatives require connection by a unifying theory. Should the EU generate a broader vision for the military and security capabilities that could be delivered by the EDTIB – a first EU "Offset" strategy?

Since assuming collaboration in defence and security is even more essential, a "dating agency" function to match nations with shared requirements into a collaborative effort becomes even more essential.
Rather than creating new organisations or agencies for the hybrid age, there already exist organisations which partially fulfil this role – like EDA or OCCAR. There are tools in place already, but they need to be used more actively (sponsored/supported by States and their MODs) and evolved, for example:

✓ CODABA database should be used more efficiently to match nations with shared requirements into a collaborative effort. These requirements/programs need to be regularly monitored and re-visited - the "baggage carousel" (metaphor used by OCCAR Director),
✓ a stronger effort for pooling of demand should be undertaken (pooling of demand V2.0),
✓ greater Involvement of industry (positive example of NIAG’s way of working)
✓ better coordination with NATO should be ensured.

Such organisation also need to be more active in advocating advantages of cooperation – highlighting the benefits such as financial savings (procurement / through life), more capability etc.

**Industry**

Industry has a major role to play in this process. Having established that "classical" defence programmes will still be required in the hybrid age, Industry needs to make them more cost effective and affordable for nation states in order to free-up budgets to meet new and emerging requirements. Generating and delivering international collaborations – that provide better value for money.

Industry (and their customer agencies) can also offer many lessons, hard-learned, from previous industrial collaborations – on governance models, common configurations, workshare and costshare etc. – that should be built upon to improve future.

Industry has a responsibility to create platforms & systems with a more open architecture for easier technology insertion/upgrade, to enable third parties involvement more easily within the defence & security systems.

For specific hybrid threats industry (major primes) need to consider adapting their business units and organisational focus to reflect the common threats & operational needs (for example regional centres of excellence).

They need to identify and build links with non-traditional suppliers for the defence sector – avoiding duplication of R&D effort from civilian sectors, instead focussing effort on the 'niche' technologies required to adapt systems to the defence domain. They also have a role to play in reducing "time to market" – more self-funded activity instead of relying on customer funding.

Hybrid warfare extends the scope of operational requirements and demands on European States. Hybrid threats are normally not aimed at one nation only and hence require a more comprehensive and multi-layer approach. Nevertheless the objectives of the EDTIB strategy remain valid but the implementation falls considerably short of expectations.
Committee 4

Trans-Atlantic and international armaments cooperation: risks, opportunities and security issues

Pilots: Dany VAN DE VEN , Paulina ZAMELEK

Members of the Committee

Norway: Johnny Asmund STOA
Netherlands: Cornel LEMMERS
Belgium: Jérôme MANISE
Austria: Norbert HUBER
Germany: Lutz KAMPMANN
Denmark: Niels Henrik HEDEGAARD
Spain: Luis Alberto MARTINEZ
France: Véronique BUSTOS (Chairman)
France: Yves-Marie GOURLIN (Chairman)
Poland: Marcin SEK
Sweden: Daniel JOHANSSON (Secretary)
Currently the two main threats perceived by most European nations are of hybrid nature: Russian behavior on the Eastern flank, and Islamist pressure from the South and South-Eastern flanks. International armament or capability cooperation could be an answer to some hybrid challenges as it may allow procuring or sharing some assets which may be best adapted to counter such hybrid challenges. The European Council also identified in 2013 the need for such collaboration (Cyber, Satcom, RPAS, and Air-to-Air refueling) and cooperation regarding Hybrid Warfare in 2015. NATO is also developing responses to nowadays threats (non-state aggressor, unconventional attacks). Trans-Atlantic and international cooperation may be linked to hybrid warfare aspects, but to counter hybrid threats it is not sufficient to focus on transatlantic or international cooperation alone.

In Europe, cooperation programs have shaped the current European armament industry landscape for decades, allowing the creation of several European industrial champions. But in recent years, the EU member states Defense R&T spending has dropped and they seem to have opted to do less together. Cooperation is a cornerstone of armament activities in Europe. It has a political, industrial, military and technological relevance in the relations among our nations, especially in the aerospace and missile domains, but also in all other armament domains.

Outside the strict European frame, there are all the other international partners which could be candidates for armament cooperation. The first of them is the USA, which benefit from a very special status because of their specific strategic position, their overall political role, industrial footprint, military capabilities (also in Europe). Many other nations are or could be partners for cooperation, and it is worth assessing, case by case, the pros and cons of a cooperative program with them.

The relation to the US is strategic for the European nations. It is challenging because of the considerable difference of power, finance, technology, and above all probably because the US want to keep an independent unrivalled supremacy according to which they are not prepared to become dependent on any nation as regards their armament. Under such circumstances, cooperating with them offers some specific opportunities but also brings a number of risks and limitations. The most significant risk probably being the risk of becoming dependent, including the risk that the US partner will abandon a cooperation program with a detrimental effect to the Europeans, as has happened in some cases. As regards other international partners, armament cooperation may still be developed, but distance, cultural difference, differing political systems and strategic interests may hamper the development of synergies, and ambitious cooperation programs could be few in number, the remaining activity being predominantly classical sales activities with possible offset aspects.

Assessing risks and opportunities of international armament cooperation also leads us to think how we could improve intra-European cooperation, in order to be less dependent on external-European cooperation. In this respect, the interest in a so-called “European FMS”, possibly based on OCCAR contracts, is highlighted. It would allow European or even non-European nations to easily procure European armament by getting orders on OCCAR contracts, getting tentatively the same serial prices and configuration as the original customer nations, and easing the process of procurement for smaller nations. Further to that, European defense research spending, with European Commission financial instruments funding and developing European key technologies, is also necessary.

European cooperation offers a lot of potential, which for the moment is not fully utilized.
Introduction – landscape

Armament cooperation is widely used in Europe, in order to share the financial burden and risk of development and industrialization among several program participants, to increase the production series, and to create a community for the in-service phase which allows achieving better through life cost (spares, technical assistance etc.). European cooperation programs have shaped the current European armament industry landscape for decades, and several European industrial champions have been created around these programs. But in recent years, the EU member states Defense R&T spending has dropped (by 27, 6 % from 2006 to 2013(1)) and they seem to have opted to do less together. The question could be raised whether there are fewer collaborative programs today than before. It seems that national political factors such as protecting local jobs and skills may be outweighing the benefits of cooperation. The member states had agreed that 20 % of R&T expenditure should be done in collaboration, but the actual figure is only 10 %. With regard to such figures, could trans-Atlantic or international cooperation be an opportunity, or a risk, for the European Defense technology and industrial base (EDTIB)? Could international cooperation reduce the risks over Europe’s defence capabilities and long term security?

In fact, international armament cooperation between European nations and third parties is mainly focused on some trans-Atlantic programs (e.g. JSF, MEADS). Armament relations with third parties other than the US are, usually and up to now, of a different nature (export of European products or transfer of a certain level of technology to third party customers). Without those exports, many European companies would be struggling to survive the cuts in their national defense expenditure.

Armament cooperation programs are often criticized for being slow and lengthy, difficult to manage due to the multiplicity of actors, and subject to over-specification due to the fact that each participating nation may bring dedicated specification elements, within program structures which are usually in a too weak position to impose compromises. However, cooperation allows developing capabilities in Europe that European nations would otherwise have to buy off the shelf, usually from the USA, and therefore cooperation allows retaining or developing highly skilled defense jobs on European soil, as well in the engineering as in the manufacturing sectors. Armament cooperation also has a political dimension which goes far beyond the pure industrial, technological and capability dimensions. Through armament programs, political ties are developed which can be important for the foreign policy of the involved nations. Armament programs usually create communities, lead to discussions at high administration and sometimes political level, and are therefore a strong factor of overall defense relations. At the same time common policies help to pave the way for more concrete cooperation including in the field of armament. Thus, this document explores what may be the perspectives offered by the trans-Atlantic and international armament cooperation, what opportunities they offer, and their inherent risks and security issues.

(1) EDA Defense Data 2013
Since the general theme of the SERA 28 is hybrid warfare, committee 4 has been studying how the topic of trans-Atlantic and international cooperation may be linked to such hybrid warfare considerations. Currently two main threats perceived by most Europeans are of hybrid nature: Russian behavior on the Eastern flank, and Islamist pressure from the South and South-Eastern flanks. International armament or capability cooperation could be an answer to some hybrid challenges as it may allow procuring or sharing some assets like reconnaissance satellites, RPAS etc. which may be best adapted to counter such hybrid challenges. But probably the whole panel of products subject to possible cooperation could be used in hybrid scenarios; as such scenarios may encompass high-intensity warfare aspects.

Worldwide developments in relation to hybrid threats:

The illustration above shows the worldwide developments in relation to hybrid threats. It shows a full range of examples which might trigger a threat. To encounter hybrid threats it is clearly not sufficient to focus on trans-Atlantic or international armaments cooperation alone.

Present technology offers access to many technical possibilities with which an individual or group is able to conduct resistance (i.e. hacking platforms, using drones as weapon platforms), and which enable them to make weapons (i.e. 3D printing, making chemical/biological bombs). To encounter a hybrid threat a multi-disciplinary approach is necessary (DIMECK: Diplomacy, Information, Military, Economics, Cultural, Knowledge) in which, on a national basis, an interdepartmental/government approach, and therefore an inter-governmental approach should be followed.
Armament cooperation with the USA

Armament relations between the USA and European nations consist in most cases of European nations buying US products off the shelf. US domestic market provides unmatched economies of scale, which often make US products attractive for foreign customers. However, other aspects also exists, may it be European sales in the USA (usually with local production, e.g. Lakota helicopters) or cooperation between US and European industrial partners (e.g. MEADS development). What have been the successes or failures of such transatlantic armament cooperation models, and what could be the opportunities and risks they offer for the future?

Opportunities with the US: FMS cases, common developments, supply chain

Off-the-shelf procurement is the most common model of European procurement in the US, in many cases through FMS. The advantages of a FMS procurement are that it can be perceived, on the short term, as very efficient: the serial price is the one of the US forces, usually rather low because the US series are big, plus an overhead linked to the US administration effort for the FMS case. The customer nation does not need to care for the program management nor for the contractual framework (except the FMS documents themselves). It’s rather simple, efficient (as the product comes from an on-going production line, the delivery timelines are usually rather short), at low program risk (the development is normally completed, the product is possibly already combat-proven). However, a FMS case usually does not allow to customize the product according to specific national needs, for instance to embark national armament, communication and encryption items, etc. Sometimes a specific contract can be placed afterwards, with appropriate industrial partners, to perform such a customization. Another aspect is the loss of sovereignty: in case of different views about foreign policy with the US, the US DoD can often restrict or even forbid the supply and / or use of the product.

An alternative way of procuring from the US is to place a direct contract with the corresponding US supplier. The advantage of such a solution is that a customization can be embodied directly in the contract. But the advantages of the FMS (no specific contract to set up, no risk associated) are lost.

As regards common development with the US, one advantage may be to benefit from the big US R&T investment, which may allow access to up-to-date technology. It may also allow concentrating the R&T effort in Europe on some domains of excellence only relying on the US in the others. The US has developed many capabilities in useful domains to counter hybrid threats (satellites and RPAS, IT/cyber/crypto). However, the US will not always grant their best technologies to foreign partners, but sometimes keep it for national use in order to maintain their unrivalled supremacy. Or, the USA will grant a privileged access to one European partner, whom they recognized as a special partner, but not to others, creating a situation where the emergence of a true European club for the corresponding product becomes impossible. Furthermore, a classical situation of mutual dependence – which could allow for a balanced and equal partnership with the US – is usually not possible because the US take care not
to be dependent on anybody when it comes to military supremacy. And as regards the IT/cyber/crypto technologies, reliance on US developed software may also bear specific risks to European nations as regards the protection of national interests as with any technology not under complete national control.

Another opportunity offered by a US partnership, at least at company level, is to be integrated in the supply chain of a US system integrator. There is a continued shift toward more systems integration and an ever increasing dependence on supply chain as a fundamental source of innovation. This is especially true when considering the introduction of new materials, new manufacturing techniques, etc., that are now more often required to produce the innovative subsystems and components ultimately needed by the system integrators to produce complex military systems.

For those reasons prospective European partners for US producers need to possess or demonstrate a willingness to invest in capabilities, technology, equipment, and personnel that enables them to deliver on the key industrial needs of the integrators. They should also have identified key areas of focus with regard to capabilities or markets where they wish to expand or have proven success. There should also be a clear understanding that, in the beginning, the partnership will involve significant time and smaller orders but that it, with success, will grow. Quality, schedule and price (in that order) will win the business. However, prospective European partners should also be aware that political disagreements between the US and their European nation wherefrom they originate may sometimes suddenly and dramatically impact their business (e.g. Iraq 2003).

**Strategic considerations associated to procurement in the US**

Besides the program advantages that procuring in the US may offer, there are in most cases political or strategic considerations associated with such procurement: US having strategic stakes in Europe may be perceived as a guarantee for US involvement in case of unrest endangering European security. And many governments in Europe find that American forces are needed to mount a credible defense in Europe. However, European nations relying on the US for their security will also have to accept the possible conditions that the US may have relating to this security guarantee. Furthermore, a "guarantee" will also risk that some EU or NATO member states will not take responsibility for their own security, including when it comes to spending on defence.

In addition, the overarching security provided by the NATO Treaty Article 5 attributes an assault of armed feature to an aggressor as a nation and corresponds with past Cold War line-up. In the light of a new hybrid approach to war, in the future NATO may have to take into account an amendment to Article 5, which would include a new or extended legal definition of aggressor and aggression to counter unconventional attacks, especially conducted by homegrown separatist militias backed by a third party or cyberassaults. However, any change proposal in the North Atlantic Treaty may encounter difficulties of political complexity nature.
One other aspect is the risk of US disengagement from European affairs, and where this could leave Europe. The US have shifted their main effort from Europe to the Asian/Pacific area, and also depending on possible changes in the US political authorities, it may be unlikely that any US government will focus on Europe as the prime US region of interest.

Considering the above, a strategic more autonomous Europe could be a goal, as well for itself (to be protected from possible changes in the US policy) as for the USA (in case they cannot or do no longer wish to pay for the dependency of Europe). More strategic autonomy in Europe may also help talking on a more peer-to-peer basis with the US. However, the inherent opportunities and risks of the concept of strategic autonomy in Europe may need to be further analyzed.

**Risks for European Defense industry regarding European procurements in the US**

Even if procurement from the US may be an efficient way to get a military capability, there are a number of inherent risks which are linked with such procurement, in the long term but also in the short term.

First of all, procuring from the US diverts significant funds from the European Defense industry, and therefore cannot contribute to improve the European serial prices. It is the case for the weapon systems, but also afterwards for their spare parts. This situation could be compensated if the US would buy in Europe in a similar way as European nations buy in the US, but it is by far not the case: even if many examples exists where the US DoD procured from a European company which had the right product at the right time, the air tankers case shows clearly that the US market in reality remains closed for European contenders, when it comes to financially significant, politically visible contracts.

In addition, procuring serial products from the US usually means either procuring the US configuration, possibly being obliged to follow the configuration management decisions taken by the US without any control on them, including the impacts on European platforms (e.g. US missiles on European aircraft, with possibly new integration / non-regression tests to be performed each time the US decide to upgrade their missiles), or procuring customer-tailored configurations for which one can negotiate the initial procurement price, but is a captive customer afterwards and is obliged, up to some extent, to accept the conditions set by the US supplier, with an extremely limited political lever on such a supplier.

Second, even when a real common program is set, the US still have the financial capability to follow several development lines at the same time (e.g. MEADS and enhanced Patriot) which may lead to unilateral US decisions to cancel a common development program, impacting very much the European partners without severe influence on the US partner. As the US always have a fallback position within the US during international technology development projects, there is a dissymmetry in the reliance on the technology. A unilateral US cancellation may lead to a stop for the corresponding activities on the European side, and possibly to a loss of the R&T knowledge developed through the program. Such a situation must be avoided, which has to be taken into account if and when considering a common program with the US.
Third, by procuring in the US, European nations accept to use the US standards embodied in the US products: this may hinder the emergence of European standards or truly common standards, and may even influence the way European nations consider warfare: as an example, the current debate in Europe about the possibility to keep a man in the loop when using an unmanned combat system may find different answers in the US than in Europe. Setting the standards, the US companies will strengthen their position which may lead to a negative circle for European businesses.

Another aspect is that an easy access to US technology kills the incentive to develop equivalent technologies in Europe (more US technology leads to less European technology and less European technology further leads to a stronger European reliance on US technology). US technology may also embody ITAR elements, which may represent a hindrance for exports.

Finally, European procurement in the US bears a long-term risk for the European defense industries; a possible way to mitigate this risk could be to invest more, and more jointly, in the European defense capabilities and at European level, in order to develop R&T and industrial capabilities more comparable to the ones in the US, and to be in a better position to negotiate with the US on a peer-to-peer basis in those areas which may be considered relevant.

NATO capabilities and stop-gap solutions

NATO being the normal vehicle of the trans-Atlantic defense relation, NATO capabilities could remain a topic for significant trans-Atlantic armament cooperation, especially in those domains where interoperability needs specific common developments. Future AWACS and AGS capabilities could be procured on the basis of a common US and European effort, but if the European defense industry wants to avoid the current situation where almost only the US industry benefits from the common NATO investment effort, the European industry should be in a position to be able to offer comparable capabilities — and to enjoy the support of all European nations.

Procurement from the US may also remain interesting to be performed for a punctual stop-gap solution, where a development does not make sense because of too small quantities to be procured (e.g. AWACS aircraft for aircraft carrier), or in order to give the necessary time to European industrial actors to develop a European solution (MALE RPAS).

On the other hand, the Libyan operation has clearly shown a European need for US support. There are still capabilities in Europe that need to be developed. In this context, the EDA and its Member States, in 2008, have developed and agreed on the Capability Defense Plan (CDP)\(^\text{(2)}\) in which among the 17 priorities, grouped in 5 different areas, there are some specially linked

---

\(^\text{(2)}\) Based on the identified trends, information gathered from Member States and the European Union Military Staff (EUMS), capability shortfall assessments, and pooling and sharing opportunities, the latest revision of the CDP in 2014 reflects a set of priority actions selected by Member States. These can be undertaken either inside or outside the EDA framework. This list of priorities is intended to be detailed enough to direct the work needed to make progress on capability development.
with the Hybrid Warfare\(^3\) (Cyber Defense, SATCOM capabilities, RPAS\ldots). These subjects have also been discussed on two European Council meetings in 2013 and 2015 respectively.

**European possible responses to trans-Atlantic armament challenges**

The attraction of FMS procurement opportunities, especially for smaller European nations, should nevertheless not be under-estimated, and corresponding answers should be designed. One possible way to counter-balance this could be to use the potential of OCCAR to offer to those European nations which request it the opportunity to procure European hardware using OCCAR contracts. The advantages for these European customer nations would be that they would benefit from the serial prices accepted by the industrial partners for the launch customers (possibly with a compensation as regards the development costs), that they would not have to worry about setting-up a complete contractual framework, as it would already exist, and that they could take part in the program management division, which gives them the opportunity to care more closely for their specific interests than they could when buying in the US.

Technology domains where national funding is scarce in Europe and where this scarcity may lead to a technology gap with the US could be top candidates for a more global European funding. One future key item, also for hybrid warfare, is the RPAS which blurs the line between direct military engagement and a more stand-off response without soldiers. But between European nations and the US, the perception of the ethical approach to unmanned armed platforms may be different. Specific European effort in this field could therefore be necessary.

Other than that, European nations have strong arguments in favor of European collaboration. These might include the cultural similarity and shared history, often comparable foreign policy outlooks, common threats and shared interests, the EU treaties framework itself and the legislation emanating from it, among others. Even though there are many advantages with European collaboration, one also need to identify the challenges.

\(^3\) EDA Future Capability Brochure 2014
Armament cooperation with other international partners

Armament cooperation with other international partners usually comes more in the form of export sales than common developments. The impacts of the economic crises have a significant effect on domestic defense spending in every European nation, and have been reducing the business base for defense contractors. This situation has increased pressure on defense companies to look more and more toward international markets to sustain their balance sheets. At the same time, foreign governments within the international marketplace are trying to find ways and means to preserve or develop their own defense industrial base as part of the need to create and retain jobs. Collaboration is seen as one of the best means of obtaining public support for spending precious governmental funds for imported defense products. This leads to having more and more transfers of technology in the armament domain.

The result is increased pressure on defense contractors to engage in more complex business relationships with foreign industrial partners in order to secure international contracts. This can mean not only partnering with a partner in the customer nation; it may well require multilateral partnerships with traditional competitors as they find themselves competing for the same shrinking market. This is just one of the challenges facing defense contractors today as they try to continue to grow in a crowded defense marketplace.

But different situation may be encountered depending on the considered nations. As a matter of classification, committee 4 has identified the following categories of possible international partners:

- Category 1: Anglo-Saxon nations: Canada, South Africa, Australia, New Zealand;
- Category 2: Asian nations, possible partners with (very) high technology level: Japan, South Korea, Singapore;
- Category 3: Emerging nations with strong industrial ambitions: Brazil, India; Gulf Cooperation Council (GCC) countries (first of all UAE).
- Category 4: All other nations.

In accordance with the tasking of committee 4, the internal European armament cooperation has not been discussed; Turkey, being part of NATO and a member in some European programs (most notably in A400M), has not been considered either.

Due to embargo reasons, Russia and Belorussia, China, Iran and North Korea have not been considered.

As a general statement, armament cooperation with all these third-party nations is normally not comparable to the type of cooperation achieved within Europe or even with the US. Opportunities may exist, usually in the frame of export cases, to perform common developments with such partners. These opportunities may be significant, especially where the third-party nations invest heavily on defense. Risks can be associated to such co-operations: creation of competitors, lack of control on the re-export of the technology, etc.
Category 1: Anglo-Saxon nations
(Canada, South Africa, Australia, New Zealand)

These nations are potential partners for common developments, because they have an overall culture as regards contracts, IPR, R&T etc. which is similar to European approaches. They have a rather similar political culture and stability when compared to European nations. The main opportunity they represent is probably to increase the launch customer basis for a given product; the main risk associated is probably that as they are very far away from Europe, a common development with them may be practically challenging. This challenge linked to distance may also exist in a US / European environment; but the existing industrial footprints of US companies in Europe or, to a lesser degree, of European companies in the US, and the existing US / European supply chains can better support transatlantic cooperation than what would currently be the case with other nations like South Africa, Australia or New Zealand.

An option is, as we do today, to propose to them developments on-site on the basis of European know-how, customized for their needs. This allow identifying win-win situations where a European company can sell its product and/or know-how but still having a significant involvement of the corresponding customer nation.

Category 2: Asian possible partners
with high technology level (Japan, South Korea and Singapore)

These nations are very interesting partners when it comes to common R&T effort, as they have a very high level of technology. But they can easily turn to become competitors; therefore any possible partnership with them has to be considered carefully if at all.

Category 3: Emerging nations with industrial ambitions (Brazil, India, GCC countries)

Brazil has high ambitions when it comes to armament industry, but its current very difficult economic and political situation makes it less probable that it will enter into new major collaborative programs in the next years. However, some industrial Brazilian capabilities are well anchored (e.g. Embraer) and should be in a position to survive the current crisis: these actors could be a starting basis for developing cooperation again, when the crisis is over.

India is a strong armament cooperation partner for Russia, and could most certainly offer cooperation opportunities for European companies. But the business environment in India is difficult and lengthy, and if cooperating with Indian industrial partners for the fulfillment of an Indian need may be thinkable, cooperating with them in the frame of a European program is not to be recommended, as it would put this European program at risk, at least time wise.

Besides Brazil and India, several GCC nations are emerging as new possible partners, also developing industrial ambitions and sustaining them with considerable financial support. On
an industrial point of view, these nations could represent opportunities for getting new developments financed.

3.4 Category 4: Other nations

Generally speaking, the armament relation to other nations will mostly be based on a simple procurement and sales basis. However, each nation is a specific case and could be assessed specifically, which no more would comply with the requirements of this document.

Some specific sub-categories could nevertheless be considered:

- Ukraine, Georgia: these 2 former soviet republics have kept significant industrial capabilities and could be partners for some projects. Their environment remains however unstable.
- Israel: having a very high technology level, Israel is usually more a competitor than a partner to many European defense businesses. Opportunities may exist.
- North African nations: sourcing in those nations may be done by some European aerospace businesses, but should instability occur, it may adversely impact the supply chains.
- Other African nations (other than South Africa and in North Africa): no real cooperation opportunity identified.
- Other Latin American nations (other than Brazil): even if some industrial potential may exist (Mexico, Chili for instance), the overall governance and economic conditions, and the distance to Europe makes it difficult to consider significant projects. But opportunities may exist, especially for developments dedicated to those nations, and should be analyzed case by case.
- Other middle-East nations (other than Turkey, Israel, and GCC): no real cooperation opportunity identified.
- Other Asian nations: many possibilities of common developments may exist in Asia, depending on the political and economic situation of each country. However, no opportunity for a reliable long-term partnership has been identified: cooperation with such nations would rather be case by case.
Conclusions – recommendations

As regards international armament cooperation from European nations with non-European nations, the USA play a special role. They play a key political and military role in European security matters through NATO and bilaterally, as an ally to the European nations, and as the main non-European supplier of armament in Europe. At the same time the US defense industry is the main competitor to the European defense companies, and even if the trans-Atlantic solidarity through NATO is a cornerstone to the European security, European nations could care about their autonomy with regards to the US\(^{(4)}\), which may affect their armament decisions.

The recommendation of Committee 4 to transatlantic armament cooperation with the US is therefore to remain pragmatic, with an open door to armament cooperation with the US (and notably where a US product can be a stop-gap solution for a capability not available in Europe), but at the same time to do more to get or maintain a more independent position in Europe as regards armament. Besides, joint capability development activities between the US and Europe will be much more viable and equitable if both sides are on reasonably equal levels.

As regards the other possible international partners, those partners who are close to the European ways of performing armament programs and who have similar objectives as regards autonomy towards the US could become long-term partners of European programs (e.g. Canada).

\(^{(4)}\) The Iraq invasion by the US in 2003 had a specific impact in those matters.
For this purpose, the Committee 4 has the following recommendations:

✓ **Research and Technology:**

- Key technologies that Europe may need should be defined at European level, by European nations, and EU funds should be invested in order to secure that these technologies will be kept and developed. This should be the core focus of the Preparatory Action(5) and of the possible defense side of the next European research program within the next Financial Framework (2021-2027). Special attention should be given to developing those technologies which will allow avoiding possible future European capability gaps.

✓ **Program management:**

- Effort should be put on the requirement definition phase, aiming at common multinational requirements instead of specific national requirements. This is a precondition to developing competitive European products with regard to US production batches.
- A common European Investment Plan (IP) strategy should be developed. First of all it would foster European cooperation; but also it would strengthen European positions by setting the rules when cooperating with non-European partners.
- Furthermore, nations should pool the acquisitions in order to produce massive orders. It would allow European industry to have a better position towards US competitors, able to discuss with others on a more equal basis. During this process the best athlete principle should be explored avoiding as much as possible damage to the already existing SMEs in Europe.
- This could be achieved through using a European body (OCCAR), which could also procure simple items for European nations. Procurement for non-European customers could also be performed by this body, with a kind of mechanism of "European blessing". A kind of "European FMS" could be created (possibly using OCCAR contracts?) in order to offer as well to European nations as possibly to non-European nations the possibility to order directly from existing contracts. For European nations developing the programs, it would allow to gain more customer nations and thus to increase the production series and to reduce their costs (including in-service costs like spares) accordingly, and also to get a part of their development and industrialization costs possibly reimbursed by new incoming customers. For European nations not participating to the initial development but procuring afterwards, it would allow to benefit from existing processes.

---

(5) The Preparatory Action (PA) is an initiative taken by the European Commission, which – along with the Pilot Project (PP) on CSDP-related research, established following an initiative of the European Parliament – could serve as an initial tool designed to create a "pilot" program of cooperation within the next Multi-Annual Financial Framework (2021-2027). This PA should provide incentive to consolidate, rationalize and increase efficiency, with multiplier effects across the European continent. As the objective is to lay the groundwork for future capability development programs, the PA should put emphasis on two main categories of projects: capability-driven research addressing commonly agreed needs, and innovation-driven research focusing mainly on those areas – such as ITAR – where Europe risks becoming too dependent on other nations (with implications on its freedom of action, security of supply and industrial competitiveness).
contractual vehicles, same serial prices (with participating conditions to be defined, as regards development and industrialization costs), and an existing program management body to which they could possibly take part. Globally, it would foster standardization and interoperability in Europe.

- Procurements from such already existing contracts, for which OCCAR could be a player, should be acceptable exemptions from the 2009/81/EC directive.

- The directive 2009/81/EC should be either better applied or changed, with the aim in any case to foster European Defense industry integration. Questionable exemptions should be assessed in this regard, and satisfactory solutions defined, taking into account the lessons learnt from the first years of use.

- Synergies regarding qualification and certification should be deepened, as it is the case with the EDA lead work on EMARs (European Military Airworthiness Requirements), with the aim to achieve at least mutual recognition of qualification / certification processes and activities wherever possible, and possibly to define European standards which would then be accepted as references for non-European customers. In the long term, synergies in the field of test centers and proving grounds could also be aimed at.

✓ Industrial policy:

- Instruments to support European Defense SME’s should be further developed, for instance by including favorable clauses when issuing European RFQs. The French model for SMEs support could be used as an example. In this model SME’s are fostered by adapted procurement practices, a long-term financial support to innovation, bilateral agreements with prime contractors and a reinforced local presence of the ministry of defence in the regions.

- Production facilities distribution in Europe should be managed so as to maximize European political support for European productions. Nations having similar objectives regarding European autonomy and interest for interoperability should more specifically join forces.

✓ Export policy:

- In order to give more efficiency to the directive 2009/43/EC and to secure European supply chains, conditions should be defined which would allow having one export decision taken by one nation also implying acceptance of other nations, at least for defined parts / components and / or for certified industrial partners.

✓ Other synergies:

- Achieving savings in other domains (by pooling of officers schools, ranges etc.) could free more funds for equipment.
### Abbreviations

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AGS</td>
<td>Allied Ground Surveillance</td>
</tr>
<tr>
<td>ARH</td>
<td>Armed Reconnaissance Helicopter</td>
</tr>
<tr>
<td>AWACS</td>
<td>Airborne Warning and Control System</td>
</tr>
<tr>
<td>CDP</td>
<td>Capability Development Plan</td>
</tr>
<tr>
<td>CSDP</td>
<td>Common Security and Defense Policy</td>
</tr>
<tr>
<td>DoD</td>
<td>Department of Defense</td>
</tr>
<tr>
<td>EDA</td>
<td>European Defense Agency</td>
</tr>
<tr>
<td>EDTIB</td>
<td>European Defense Technological and Industrial Base</td>
</tr>
<tr>
<td>FMS</td>
<td>Foreign Military Sales</td>
</tr>
<tr>
<td>GCC</td>
<td>Gulf Cooperation Council</td>
</tr>
<tr>
<td>IPR</td>
<td>Intellectual Property Rights</td>
</tr>
<tr>
<td>ITAR</td>
<td>International Traffic in Arms Regulations</td>
</tr>
<tr>
<td>JSF</td>
<td>Joint Strike Fighter</td>
</tr>
<tr>
<td>MALE</td>
<td>Medium Altitude Long Endurance</td>
</tr>
<tr>
<td>MEADS</td>
<td>Medium Extended range Air Defense System</td>
</tr>
<tr>
<td>OCCAR</td>
<td>Organisation Conjointe de Coopération pour l’Armement (Joint Organisation for Armament Cooperation)</td>
</tr>
<tr>
<td>PA</td>
<td>Preparatory Action</td>
</tr>
<tr>
<td>R&amp;T</td>
<td>Research and Technology</td>
</tr>
<tr>
<td>RFQ</td>
<td>Request For Quotation</td>
</tr>
<tr>
<td>RPAS</td>
<td>Remotely Piloted Air System</td>
</tr>
<tr>
<td>SATCOM</td>
<td>Satellite Communication</td>
</tr>
<tr>
<td>SERA</td>
<td>Session Européenne des Responsables d’Armement (European Session for Armament Executives)</td>
</tr>
<tr>
<td>SMEs</td>
<td>Small and Medium-sized Entreprises</td>
</tr>
<tr>
<td>UAE</td>
<td>United Arab Emirates</td>
</tr>
</tbody>
</table>
Committee 5

European Defence Research: how to cope with hybrid threats and new challenges in 21st century “warfare”?

Pilots: Alfred VOGEL, Olivier GRAS

Members of the Committee

Ingo WACHS
Jean-Didier VANDEZANDE
Christian STEINO
Jose Agrelo LLAPEROL
Laurent BOULOIGNE
William POINTING (Secretary)
Larisa POGRAJC
Mikael KRUSENBERG (Chairman)
Topias OLLILA
Antonio PANTALEO MANIGLIO
Slawomir PACZEK
Gentlemen, we are out of money. Now we have to start thinking.
(Winston Churchill)

Committee 5 (The Committee) identified the key components of Hybrid Warfare and determined that its nature was dynamic and evolving. This was a result of the development of the ways and means of conflict by both state and non-state actors. The main issue is that adversaries are exploiting, and will continue to exploit, existing and emerging technologies to operate below European nations’ current decision-making (and action) thresholds. It is therefore necessary to develop R&T activities that would provide Europe with the capabilities required to reduce the span of choices available to potentially hostile "hybrid warfare" actors. R&T activities should be driven by the active analysis of existing and developing threats.

The Committee identified that there were areas of overlapping strategic security interests within Europe and there were therefore opportunities for specific groupings, working within a lead-nation framework to prosecute common R&T activities. There were existing examples within the European construct, such as the European Space Agency, which might provide the basis (or an exemplar approach) for the development of future European R&T activity.

There remains a risk that R&T will continue to be duplicated across Europe in order to meet national strategic or industrial policies and the Committee further identified that the European Defence Agency (EDA) might provide a common forum to allow nation states to identify areas of common interest and then to gather funding and support from like-minded nations. This process would be on an "opt-in" basis. There was, however, a need for pragmatism about the ability of the EDA to manage the effective delivery of R&T across a large number of nations and it was assessed that it was unlikely that workable levels of agreement could be reached across a large (greater than 4) number of nations.

The Committee identified a number of areas that might be suitable for bilateral, multilateral or (very rarely) pan-European approaches to R&T.
The exam question

Committee 5 is to elaborate a ‘food for thought’ paper proposing guidelines about Defence Research and Technologies (R&T) needed in countering hybrid warfare while keeping also in mind those needed for high intensity operations.

Approach. The Committee will conduct a Defence and armaments related appreciation focused into the European Union Preparatory Action (PA) that will serve as a testing ground for a future dedicated EU CSDP related Defence-orientated R&T and will illustrate the ‘value added’ of an EU contribution in new R&T areas noting that;

✓ The Preparatory Action will last for a maximum of 3 years.
✓ And, if successful, the PA will pave the way to an EU-funded Defence Research Programme (ERDP) within the next Multi-Annual Financial Framework 2021 – 2027.

Hybrid warfare – the context

Hybrid warfare can be characterised as being primarily about state and non-state actors seeking to operate below an adversary's threshold (ability or desire) to respond. The current focus on hybrid warfare arises, to a large extent, from the inability of European nations to be seen to proactively counter emerging threats from both state and non-state actors. Governments are, at the same time, struggling to reduce the impact of violence within their own territories and to maintain the rules-based approach to the conduct of international relations between states. The Committee determined that it is easier for autocracies, kleptocracies and theocracies to plan and prosecute hybrid warfare strategies than it is for European nations to be able to counter these threats effectively.

Asymmetry, Deception, Information and Psychological Operations

There is, however, little that is new about the evolving nature of the use, or threatened use, of force to achieve comparative advantage between state and non-state actors. Components of

---

(1) Defence Research and Technology (R&T) expenditure: expenditure for basic research, applied research and technology demonstration for defence purposes. It is a subset of R&T expenditure. Source is: http://www.eda.europa.eu/info-hub/defence-data-portal/definitions. This paper further assumes that R&T can support the analysis and improvement of systems and decision-making processes.

(2) The EDA published texts describing the PA that are partially reproduced under paragraph 23, for completeness. Source is: http://www.eda.europa.eu/what-we-do/activities/activities-search/preparatory-action-for-csdp-related-research.

(3) Russian doctrine regarding Information war can be defined as: confrontation between two or more states in the information space to damage the information systems, processes and resources (which are of critical importance) and other structures, to undermine the political, economic and social system, and effect massive brainwashing of the population for destabilizing the society and the state, and also forcing the state to make decisions in the interests of the confronting party.
the hybrid approach can be found in the analysis of previous conflicts and operational techniques across time. Examples include:

✓ The writing of Sun Tzu i.e. "Let your plans be dark and impenetrable as night, and when you move, fall like a thunderbolt"[4].
✓ The entrapment and surrender of the Roman Army at the Caudine Forks[5].
✓ Development of Iranian Revolutionary Guard Corps (IRGC) strategy to defeat the USA in the Lebanon in 1983 through the sponsoring, development, training and supply of Hezbollah.

Current Use of the Term "Hybrid Warfare"

Hybrid warfare is not a new term; it was used in 2002 in a thesis written by William J Nemeth at the US Naval Postgraduate School (Future War and Chechnya: a Case of Hybrid Warfare)[7]. Despite this, the term "hybrid" has, until recently, been little used in national or NATO written analysis of Security issues;

✓ The latest NATO Strategic Concept (2010) does not, for example, mention the term "hybrid".
✓ The UN has equally been slow to adopt the term and usually refers to "asymmetric threats" – which is a component of hybrid conflict – but does not use the term "hybrid".
✓ The term has, however, begun to gain currency; NATO used the term "hybrid" in 2014 at the Wales Summit of 5th September 2015 which followed the Crimea and Ukraine. The final declaration of this Summit refers to "hybrid warfare threats" where a wide range of overt and covert military, paramilitary and civilian measures are employed in a highly integrated design[8].
✓ A graphical representation of the phases and lines of operation that enable hybrid warfare is at Page 95.

The Threshold

Hybrid warfare occurs because, it can be argued, adversaries are unable to achieve their policy objectives through more traditional high-intensity warfighting operations; if adversaries believed that they could be successful through overt armed action then many might, out of preference,
use this means. There is, therefore, an imperative for European states to maintain traditional warfighting capabilities in order to deny this approach to adversaries and at the same time to develop ways and means to reduce the potential hybrid approaches available to state and non-state actors.

Characteristics

The characteristics that define hybrid warfare can be described as having the following elements within which an adversary seeks to destabilise the leadership and the civil society of European nations to provide them (the adversary) with increased freedom of action and operational and tactical choice:

✓ Temporal. An adversary will seek to act faster than European nations can react.

✓ Legal. An adversary will seek to act in a manner that cannot be matched within European nations’ legal or political limitations which are constrained by the need to adhere to national and international law.

✓ Ethical. European nations, as a result of their current democratic nature and liberal democratic histories, are less able to plan and operate within the levels of freedom (within psychological and information operations, for example) that adversary state and non-state actors are able to do. This places European nations at an operational and tactical disadvantage as they are less able to deliberately conceal their strategic intent.

✓ Societal. An adversary will seek to exploit an adversary’s societal aversion to offensive or anticipatory actions.

✓ Pain or Loss. An adversary will seek to operate below the (pain) threshold at which an adversary’s loss triggers societal or political pressure to react decisively.

Multi-Layered Problem

Hybrid Warfare therefore presents a multi-layered problem to European nations who, in recent history, have largely been confronted by an essentially monolithic threat in the form of the Warsaw Pact. More recently they have assumed that security can be delivered through the construction and maintenance of effective international institutions. The current state and non-state actors are now demonstrating an ability to operate in an integrated fashion across the full spectrum with the aim of creating ambiguity and confusion on the nature, the origin and the objective of the threat. The range of potential threats includes:

✓ “Posturing’ with nuclear weapons drills and deployments.

✓ Access Denial and long range strike capabilities that will prevent European nations from deploying forces to support allies or concentrating force to deter attack.

✓ “No notice’ large scale exercises and drills in border regions.

✓ Comprehensive use of long term soft power: language schools; media operations; promotion of the aggressor’s power culture among target populations; social media trolling
and rumour generation.

✓ Offensive cyber operations including denial of service attacks and degradation of infrastructure and Government services.

✓ “Plausibly deniable’ deployment of Special Operations Forces (SOF) and intelligence services to generate “local’ armed action.

✓ The deployment of unmarked armed forces – little green men.

✓ The planning and exploitation of criminal activity and terrorist/terror actions.

Considerations

Balancing Security and Defence Activities

European societies are unlikely to commit significantly-increased funding levels to Defence forces, albeit that some are beginning to increase spend on internal and external security structures and capabilities. As Governments are attempting to identify how best to reduce the vulnerabilities open to potential adversaries many are shifting to a Joint and Inter-agency operating model to enable them to better deal with the threats posed by Hybrid Warfare. There is therefore a need to determine how best to optimise expenditure; and to do so in an increasingly agile and dynamic manner to treat a series of perceived or actual threats as they emerge from a continuously reviewed and updated analysis of one’s own vulnerabilities.

Differing National Approaches

Having identified that there is a compelling need to optimise spend (through capability sharing or specialisation) for R&T and “action’ across Europe; Committee 5 identified that there are a number of differing national approaches that have conspired to create overlaps in R&T activity and to reduce the effectiveness of existing expenditure. These differences can be summarised as follows:

✓ Sovereignty. All nations maintain, to one degree or another, national sovereignty over key capabilities and force elements.

✓ State Industrial Policy. There are differing national approaches to Defence R&T planning and execution both in terms of the agility of R&T plans and programmes and the degree to which Defence R&T is closely (or loosely) linked to wider governmental research.

✓ Defence and Security Planning. Nations have different approaches to linking Defence expenditure and capabilities to internal security capacity and, as a result, may be unwilling to share what appear to be primarily Defence R&T products.
National Prioritisation of Threats

Discussion in Committee 5 has identified that European nations have differing perceptions of the relative prioritisation of the threats that confront them.

Graphical Representation
A description of the differing levels of threat perception by 3 “illustrative’ nations is shown below as graphical example:

Causes
The causes of these differences in perception and prioritisation are to be found in geographic location, recent national histories, differing national strategies and objectives, and differing views of the role of NATO (and other international alliances) in national defence planning.

So What?
There are very few areas where all European nations can agree on the relative prioritisation of the threats to their national security and it is equally unlikely that all nations will be able to agree on the same prioritisation for R&T activities. There is, therefore, a need to plan and conduct R&T on the basis of smaller groupings of nations who share similar views about common threats.

Differing National Levels of Threat Perception
Potential Ways and Means

Committee 5 determined that the result of R&T and the exploitation of novel technologies was part of a wider European approach to counter hybrid threats. This approach should seek to: decrease a potential adversary’s freedom of action during the preparatory phases; increase the range of credible responses available to European nations; and improve Europe nations’ ability to act decisively to pre-empt or counter detected threats. The potential "ways and means’ include:

✓ Long term cultural "influence’ of target populations.
✓ Political "messaging’ to adversary nations/entities.
✓ Development of national (most likely) or multi-national (less likely) ability to identify, adopt and deploy rapidly emerging (COTS) technologies or novel uses of extant technology.
✓ Establishment of multinational standards and information-sharing systems to enable collaborative detection of threats/attacks including: economic; CBRN; and cyber.
✓ Exercises and rehearsals at national and multi-national levels to confirm/develop tactics, techniques and procedures (TTPs).
✓ "Show of force’ exercises and drills.
✓ The forward deployment of assets/force elements.

The Value-Add of a European Approach to R&T

Committee 5 identified the following benefits of improving European Defence-related R&T capabilities.

✓ To Enable European Strategic Autonomy and Security of Supply.
✓ Reinforcement of European Cooperation. The integration of elements of European R&T activity should help to further stimulate and support the development of bilateral and multilateral defence capabilities.
✓ Coherence with Strategy. There is an opportunity to employ the better alignment of European R&T activity to help shape the emerging European Defence Strategy.
✓ Smart Defence. Declining defence budgets across Europe and the pressures imposed by the need to support internal security and counter-terrorism should drive European nations to align R&T activities so that R&T outcomes are delivered more efficiently.
✓ R&T Effectiveness. There is, it is assessed, a considerable degree of overlap in R&T spending and activity across Europe which does not adequately exploit centres of excellence or enable the most efficient exploitation of previous expenditure.
✓ Maintaining and Broadening the European Industrial Base. Improved European R&T should enable the maintenance of the scale and scope of the existing European Defence industrial Base and to broaden it into new areas, including cyber.
The European Space Agency (ESA) – an Exemplar for Wider R&T Funding?

Discussion within Committee 5 identified that the ESA might provide a working model to shape our approach to future R&T cooperation. The ESA has created a European space strategy and developed an effective approach to the funding and execution of the associated R&T.

Outline ESA Approach to R&T

1. ESA has compartmented its R&T activities into different domains, i.e. launchers, science or earth observation.
2. R&T activity in each domain is then planned against a multi-year schedule.
3. Each nation contributing to ESA then defines its level of investment for each capability. Funded programmes are able to be initiated with confidence that they have the appropriate level of funding.

✓ Juste Retour\(^5\). A participating nation is guaranteed that their national industries will be contracted to deliver work to ESA in proportion to its investment. There is therefore a direct link between public investment and industrial jobs in each country.

✓ Benefits. The benefit of this approach is that Europe is able to compete globally as the provider of space services and capabilities, albeit that the funding mechanism drives a degree of inefficiency into the overall programme costs.

✓ Risks. Care will need to be taken, however, to ensure that selected topics are likely to attract and retain enduring funding and support. The experience of the Capability Technology (Cap Techs) activity has exposed the difficulty of creating consistent and sustained national support for specific projects.

---

\(^{(5)}\) Principle that the funding granted to project participants from a given country/region under a joint call is in proportion to the budget contributed to the joint call by that country/region. Source: https://www.era-learn.eu/service/glossary/juste-retour.
Answering the exam question
Achieving distributed/shared European R&T

Committee 5 resolved that European interests do overlap and that there is scope for the optimisation of R&T spend. There is, however, a need to understand and respect different national approaches if we are to construct a credible, deliverable forward R&T approach.

✓ Some nations will be very comfortable with long-term technological programmes, others better suited to shared innovation and exploitation of emerging technology – there are, inevitably, horses for courses.

✓ There is a need to identify sub groups of nations with similar threats/concerns and encourage/enable them to act together.

✓ One size will not fit all and MBDA’s experience shows that change is a 20 year journey; we need to get started.

✓ There is a need to use the opportunity presented by “Preparatory Action’ as a “pilot’ to test what will work (and what will not).

Potential Guidelines

It will not be possible to arrange and fund R&T activities that cover the full spectrum of capabilities required to counteract a hybrid threat, it will therefore be necessary to focus funding and activities by applying the following guidelines:

✓ Identify discrete areas of R&T which will benefit from the engagement of a defined number of nations with common interests and a common perception of the key threats to them.

✓ Focus on funding R&T for Defence purposes.

✓ Identify how to exploit rapidly existing or emerging technologies that are created by civilian or commercial R&T activities.

✓ The Committee judged that the selection and sustainment of a lead nation will be important to the success of individual R&T projects.

Potential role of the EDA

Drawing on discussions relating to the ESA, Committee 5 identified that the EDA might act in a similar manner both to coordinate national funding for R&T projects and to provide a forum for the brokering of multinational and bilateral R&T projects. The key components that would need to be put in place are:

✓ The preparation of a European Defence Strategy within the construct of CSDP.

✓ Agreement on the principal of Juste Retour.
✓ The adoption of a Lead Nation concept for specific projects.

✓ A quarterly (4 times in each calendar year) review cycle to ensure that R&T investment and exploitation remains appropriately prioritised to meet emerging threats.

With regards to the PA, Committee 5 acknowledged a significant role for the EDA as the forum for MoD strategic dialogue leading to their mutual cooperation.

**Potential R&T Topics**

Committee 5 determined that it would not be possible to cover fully all of the potential areas for R&T and therefore selected a number of topics that might be considered within the Preparatory Action. These topics are summarised below and described in more detail in the following pages:
Generic Russian Operational Framework

(10) From page 45 of Fear, Honor, Interest: An Analysis of Russia’s Operations in the Near Abroad. A monograph by Maj Antonius JC Selhorst, Royal Netherlands Army, School of Advanced Military Studies United States Army Command and General Staff College Fort Leavenworth, Kansas. AY 2015-001.
European commission preparatory action

Cooperative defence research programmes are essential for sustaining and fostering key military capabilities in Europe, and for addressing capability shortfalls. The European Commission plans on launching a Preparatory Action (PA) on CSDP-related research with a view of inserting a thematic area on CSDP-research in the next framework programme, after Horizon 2020, in support of European defence cooperation and of the European defence industries. EDA, as the hub of defence research at EU-level is a natural partner of the Commission in the preparations of both the Preparatory Action and its follow-on programme in the next multi-annual financial framework. Therefore the Commission and EDA organise consultation meetings with the Member States, in the form of workshops, to discuss the main questions of the PA.

Project activities

✓ Organise consultations with the Ministries of Defence of the 27 EDA Member States.
✓ Consolidate the views of the Member States in order to build a solid research programme for CSDP.
✓ Provide views to the European Commission for the launch of the PA in 2017.
✓ Beside the workshops, set up topical working groups on complex sub-issues, such as the IPR scheme (Intellectual Property Rights Scheme).

Project objectives \(^{(11)}\)

✓ Addressing the current decline in European defence R&T by boosting investment
✓ Addressing core future technology needs where economies of scale exist and reducing duplication
✓ Strengthening the long-term competitiveness of the EDTIB throughout the supply chain
✓ Building on significant European competences, including the innovative potential of SMEs
✓ Complementing and supplementing existing national and collaborative efforts

Detailed description of the project

EDA and the European Commission recognise that investing today in future-oriented defence research programmes is crucial to developing the capabilities that are required tomorrow. The Commission, which currently finances exclusively civilian or dual-use R&T through its 80 billion € Horizon 2020 programme, considers the Preparatory Action as a major instrument for testing the added-value of CSDP-related research within a permanent EU framework.

If successful, the Preparatory Action could pave the way to a fully-fledged EU defence R&T programme within the Multi-annual Financial Framework (MFF 2021-2027). The key aspect in assessing the added value will certainly be the uptake of the technology research by the industry and the Ministries of Defence which will ensure the production of new strategic capabilities for armed forces in Europe and increase the competitiveness of the European defence technological and industrial base.

The Preparatory Action will be launched in 2017 before becoming part of the MFF 2021-2027. A certain number of questions related to implementation modalities still need to be worked out before the launch of the programme:

✓ Decision mechanism on the work programme.
✓ Evaluation of the proposals.
✓ Rules for participation.
✓ Funding scheme.
✓ IPR scheme.
CBRN - Biological

Initial Analysis - Emerging CBRN Threats

The Globalisation of technology will lead to greater proliferation of lower-end equipment and a reduction in its cost. This will allow a wider range of actors’ access to comparatively sophisticated weapons. Existing dual use or commercial technologies could be employed in highly innovative ways, which may be disruptive(1).

It is realistic to expect more CBRN threats in future. Potential biological weapons pose a threat with possible serious consequences, could be relatively accessible, inexpensive and difficult to defeat.

Any country with microbiological laboratories is capable of producing pathogens, but there is also the risk of the natural spread of infectious microorganisms (i.e. various epidemics). The consequences will be much broader than just the effect on the health of the population; it will have economic, social and other impacts of society.

Possible conventional and new biological threats

Biological warfare can be defined as the deliberate use of microorganisms and toxins, generally of microbial, plant or animal origin, to produce diseases in humans, animals and plants (DaSilva, 1999)(2). This definition, whilst comparatively recent, is already outdated. It does not take into account newly emerged and emerging technologies such as nanotechnology, biotechnology or synthetic biology for instance. Emerging biological threat is more diverse in nature; it can affect not only human beings, but also disrupt economic systems and create chaos(3).

We can divide biological threats into two categories: conventional biological threats and threats of newly emerged or emerging technologies. Another division, according to modus operandi, is into acute and less detectable (subtle) agents(4), where acute agents are more similar to our perception of conventional type whilst subtle to new threats, although even conventional could be subtle.

- Acute agents include those that can cause severe illness very rapidly, which usually leads to death without (or even with) treatment.
- Less detectable agents cause disease over a longer period, from months to even decades, enhance vulnerability and / or economic disruption through impact on water and food supply, impairment of a population’s abilities to function due to illness that affects specific organs in the human body(4).

The globalisation of knowledge which is easily accessible through modern media is making break-through technologies relatively easy accessible for potential misuse. Diseases could be in future spread through unconventional agents like e.g. nano-particles. Some of them are known to cause severe respiratory difficulties and related illness. Rapid development of gene technologies can lead to the creation of genetic weapons. Genetically modified organisms (GMO) present a broad spectrum of possible applications in pharmacy, medicine, agriculture etc. Misuse of them in the field of agriculture and water supply can lead to catastrophes of large dimensions. The rapid detection and treatment of even well-known “conventional” microorganisms is very demanding, but fast in-situ detection of GMOs with appropriate preventive measures poses a scientific challenge. Fast and sensitive detection is crucial for the implementation of effective preventive measures.

Synthetic biology is modifying the DNA of an organism to change its information contents, such as selecting desired mutations, inducing mutagenesis, altering genes or regulatory elements, cloning, designing biological components and systems that otherwise do not exist naturally. It provides the tools to “redesign” the genomes of existing microbes to increase their efficacy or provide new functionalities\(^5\). Such re-designed micro-organisms could be tailored to enhance virulence or be resistant to known medicine. Their incorporation into the human body or into crops or water could make a contaminating agent extremely difficult to deal with.

Speed and methods of dispersion and transmission in the environment are critical for evaluation of a potential bio-threat. With new emerging technologies, new methods of dispersion and transmission are possible such as use of different new vectors (e.g. insects, nano-particles). Just as new technologies can be misused, they can as well be used to defend efficiently against new threats. Potential fields of application are limited only to our imagination: new crops, new effective medicine, personalised medicine, technologies that enhance human health, especially immunity and cognitive performance etc. Inevitably, most of these fields will create new ethical issues.

### Proposed research areas

Below are listed some of the identified and proposed future research areas directly or indirectly linked to new emerging CBRN, especially bio-threats:

- Nanotechnology
- Biotechnology
  - Genetics
  - Synthetic biology
- Microbiology
  - Vector threats
- Pharmacy (new drugs – treatment and prophylaxis)
- Real time sensitive detection methods
- Sensor development
  - Micro, nano and enhanced sensitivity
  - Specific contaminant signatures
  - Sensor platforms
- Systems to enhance human (physical and cognitive) performance
- Personal protection equipment
- Remote systems
- Automated systems
- Austere environments
- Big data analytics
- Ethics

### European Union’s future R&T on biological threats – a possible way forward

The EU is, and will undoubtedly be increasingly, faced with new hybrid biological threats. To defend against them we need a shift in both our thinking and ability to exploit technologies – a new concept is needed. There are a number of key questions:

- What is the role of European research and technology (R&T) now and in the future?
- How can R&T contribute to a safer and more secure Europe?
- How fast is it possible to react within the R&T domain?
- Can cutting edge European science and technology represent a solid base to enable our ability to anticipate the unexpected?

---

There will be other questions that emerge but answers to them are not as obvious and uniform as one would wish. It is clear that we do not have a lot of time to react—nor least because scientific research usually takes time.

To successfully defend against emerging bio-threats a cutting edge science and technology is needed but limited, and reducing, funds for R&T has also had a negative impact on defence research. How much can we and are we prepared to increase funds for defence R&T? Reality may force us to do so, but an increase in funding may not be sufficient and we will need to explore different approaches.

**Balancing Civil and Military Research**

Research into bio-threats is predominantly dual use in nature. A number of excellent research institutions within Europe deal with research areas directly or indirectly linked to CBRN threats.

Civil research represents at least a base of lower technology readiness level (TRL) research while typically defence research could be follow-on, oriented into higher TRLs. Combining the two will concentrate time and resources. Although higher TRLs will give results in a more convenient time period, a balance between basic research and high TRL product oriented research should be maintained in order to assure research sustainability.

**Economic Interest – Involving SMEs**

Since coping with new bio threats is demanding, high tech products with higher added values and a need for the fast evolution of these products better suit adaptable small and medium enterprises than bigger ones. Although the economic interest of each member state is important, it should be incorporated but not prevail over a common EU defence interest. EU competitive advantages should be found and developed towards excellence instead of competing with high technological and scientific societies like US in all areas. Research activities should not be extensively spread among research institutions within EU and should not be duplicated with NATO, although some healthy competition could remain. Technology watch should be done on regular basis both within the EU and more widely.

**Prioritisation**

Because of the urgent need for rapid response, there is a need to develop a priority set of short-term and medium and long-term research activities within the EU supported by a higher political consensus.

*Some threats have not been operationalized even if the capacities already exist. If they will emerge sooner or later or at all is for the future to decide; the only sure thing about the future is that something unexpected will occur.*

<p>| Comment on suitability for pan-European approach and/or allocation to sub-group | Suitable for pan-European approach including dual-use research. |</p>
<table>
<thead>
<tr>
<th>Subject</th>
<th>Detail</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Initial identification of the threat/capability</td>
<td>Counter UAS</td>
<td></td>
</tr>
<tr>
<td>Initial analysis</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Threat.** The numbers of unmanned aerial vehicles (UAVs), or drones, are multiplying rapidly. Missions for these small unmanned aircraft are as diverse as crop monitoring and filmmaking, but UAVs used with malicious intent constitute a growing threat both on and off the battlefield. UAVs are seen as a new threat because of their low cost and ease of use. Small UAVs are proliferating rapidly and are an increasing threat to public safety - not only to Commercial Air Traffic and to conduct Industrial Espionage but also to the soldier on the battlefield where UAVs are seen as the new IED.

Increasing incidents of drones flying over sensitive facilities, including nuclear reactors and airports, has spurred demand for systems to keep them at bay. As the sale of commercial and private drones increase, so are instances of them being flown in areas they shouldn’t be.

**Response.** Governments will have to find ways to control the use of aerial drones through regulation, physical detection and denial or a combination of these means.

**Definition. UAV, UAS or LSS?**

A UAV can be defined as a “powered, aerial vehicle that does not carry a human operator, uses aerodynamic forces to provide vehicle lift, can fly autonomously or be piloted remotely, can be expendable or recoverable, and can carry a lethal or nonlethal payload” (Wikipedia)

UAVs differ from ordnance and missiles in that the air vehicle is designed to come back and be re-used. They also differ from remotely-controlled aircraft and especially small hobby planes in that they operate out of line of sight and at altitudes where a person on the ground cannot readily see them. Like guided missiles UAVs are sophisticated systems incorporating lightweight airframes, advanced propulsion systems, secure data links, and high technology control systems and payloads. These air vehicles still need a pilot who rather than being seated in the aircraft itself is located in a control centre normally referred to as a Ground Control Station.

The term Unmanned Aircraft Systems (UAS) may therefore be a better definition that is more relevant as ‘UAV’ refs to the vehicle itself whereas ‘UAS’ describes the vehicle, its guidance system and the mission payload. UAVs or UAS will in the future become fully autonomous. Like advanced artificial intelligence these systems will be able to sense where they are, what they are doing, what they should be doing, where they should go to complete the pre-programmed task and how they can complete that task most efficiently and effectively and with a certain degree of luck return to base. In the future the UAS rather than the UAV pilot will be the biggest decision-maker during a mission with the UAV pilot increasingly being employed to monitor what the vehicle is doing.

Characteristic when talking about UAS is that they are small, slow and operating at low altitudes hence often referred to as Low, Small and Slow (LSS). These characteristics are very important when discussing the area of R&T.

**The Kill Chain.** The kill chain for C-UAS is similar to the classical air defence kill chain, involving the requirement to detect and track the aircraft, identify whether it’s a threat, determine a course of action and then engage the target. In the case of the C-UAS mission, multiple sensors, including radar, EO/IR cameras and Electronic Warfare (EW) equipment to provide detection, tracking and identification are necessary. Defeat (C-UAS) may include traditional kinetic anti-aircraft systems, directed energy weapons, EW techniques, etc.
# Areas of interest

Three areas of R&T interest can be defined:

- Detection. As UAS are LSS they pose a new challenge in traditional detection systems as radar. But also EO/IR detection pose problems due to the UAS small form factor.
- Identification. How can UAS be identified?
- Defeat. How can UAS be defeated?

## Proposed approaches to research

Research should be centred on the three areas of interest - detection, identification and defeat.

- Radar should be optimized to look for LSS and due to the rapidly increasing numbers of available UAS; radars should be developed to be small, ultra-mobile and inexpensive.
- Other, non-radar, sensor systems to detect LSS should be researched.
- How can LSS be identified and distinguished from (for example) birds?
- How can LSS be defeated? By kinetic anti-aircraft systems, directed energy weapons, EW techniques or other?

## Comment on suitability for pan-European approach and/or allocation to sub-group

As the challenges UAS pose to society are global, Europe could greatly benefit from combined research.
### Initial identification of the threat/capability

**Counter Improvised Explosive Device (IED).**

The employment of increasingly effective IEDs has proliferated in recent years and counter IED capabilities are now essential for operations even in sub-Saharan Africa and other less-developed parts of the world.

There is therefore a need for European governments to be able to defeat IEDs both to provide force protection to deployed force elements and to sustain domestic support for deployed operations.

### Initial analysis

Counter IED capabilities are specified for NATO operational purposes and are also the subject of NATO and EU groups standardization analysis. R&T on C-IED capabilities is also carried out by individual countries.

**Components of the C-IED Capability.** C-IED capacity is the result of the coordination of military and civilian capabilities in the following areas:

- WIT – Weapon Intelligence Team,
- EOD – Explosive Ordnance Disposal,
- TECHINT – Technical Intelligence,
- HUMINT – Human Intelligence,
- FABINT – Forensic and Biometrics Intelligence
- CIMIC – Civil and Military Cooperation.

The results of the combined analysis of the products of these organisations will allow the development of C-IED concepts and doctrine and military and technical requirements.

### Areas of interest

- Advanced Sensors
- Data collation, integration and fusion system
- Transition of data into information and intelligence suitable for decision-making

### Proposed approaches to research

Research should be focused into the following areas to enable C-IED equipment to meet the following functions/capabilities:

- to recognize an attack and to conduct actions against attacks;
- to prevent IED attacks by the development of effective operating and technical procedures;
- to detect IEDs;
- to neutralize IEDs;
- to reduce/mitigate the effects of the IEDs use;
- to utilize information and experience to further develop C-IED capabilities.

### Comment on suitability for pan-European approach and/or allocation to sub-group

Equipment to be obtained in the framework of research and development (R&T) are as follows:

- Different categories of engineering works, including the recognition of roads and buildings;
- Mine-sweep equipment;
- Electronic jamming (electromagnetic interference) equipment;
- Protective clothing;
- Mine clearance and inactivation IED equipment.
### Initial identification of the threat/capability

**Detail**: Defeat of Anti-Armour Missiles.

### Initial analysis

**Threat**: There has been rapid proliferation of advanced anti-armour systems to state and non-state actors (including Hezbollah) in recent years. There is an increasing need to defeat modern anti-armour systems in the congested, cluttered and contested environments that characterise Hybrid warfare operations.

**Response**: It is therefore necessary to bring to maturity new technologies that provide soft and hard kill Defence Aid Suite (DAS) systems that are employable with low collateral damage.

**Technological Capabilities**: Areas for the development of DAS include:
- Defeating attack by multiple missiles.
- Multirole optimization including:
  - anti-ground and anti-air,
  - multitarget tracking,
  - jammer rejection from multiple directions,
  - clutter rejection,
  - aiming point selection on the target,
- The adoption of Active Electronic Scanning Antenna Seeker (AESA) able to defeat missile sensors.
- Direct Energy Weapons (DEW) based on Laser Direct Energy Weapon (LDEW) and/or high Electromagnetic Pulse (EMP) to defeat incoming missile threats.
- Offensive Cyber warfare to create the ability to interfere with threat missile guidance systems.

### Areas of interest

**Associated Technologies**: Areas for research include:
- System autonomy (Artificial intelligence, Automatic Target Recognition, Cooperative Engagement Capability);
- Laser technologies for Direct Energy Weapon systems;
- Conformal AESA Antennas;
- Materials for energy storage
- Future Missile data links for UAV weaponization;
- Power Switches;
- Laser Actuated Igniters;
- Data link;
- Navigation and control

### Proposed approaches to research

**Development of a Common Technology Road Map**: In order to counteract emerging missile/anti-armour threats a common technology road map at European level could be developed to increase Technology Readiness Levels:
- **Short Term**: The development of a common Technology Demonstration Programme (TDP) achieved through experimentation.
- **Medium Term**: The conduct of common research activities to develop prototypes for a new generation of defence systems in this domain.

**Defeat of Attack by Multiple Missiles**: The future missile/anti-armour threat may be defeated by increasing both the hard kill and soft kill capabilities. An important area for further development is the defeat of an attack by multiple missiles. The systems to be developed include: multirole capacity for anti-ground and anti-air; multi-target tracking; jammer rejection across a broader sensor aspect; clutter rejection; aiming point selection on the target; and more effective war heads.
Improvement of Hard Kill Systems. Hard Kill DAS could be improved by the adoption of:

- **Active Electronic Scanning Antenna Seeker (AESA).** The development of AESA technologies to achieve the defeat of attacking missile sensor systems.

- **Improved Warhead Technologies.** The development of new energetic and reactive materials that have greater lethality than current war heads of similar weight.

**Development of Soft Kill Systems.** Potential soft kill systems include the technologies inherent within Directed Energy Weapons (DEW) including Laser Directed Energy Weapon (LDEW) and High Power Electromagnetic Pulse weapons. Both systems are able to defeat an incoming missile threat before it reaches its target.

<table>
<thead>
<tr>
<th>Subject</th>
<th>Detail</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Initial identification of the threat/capability</td>
<td><strong>Area Denial and Anti Access Capabilities.</strong> The Proliferation of Area Denial and Anti Access Systems. Russian military expenditure has increased and is allowing the development and deployment of long range ground to air and ground to ground systems that will limit European Nations confidence ability to operate air systems (including ISR platforms) and the successful use of fixed facilities including ports and storage facilities.</td>
<td></td>
</tr>
<tr>
<td>Initial analysis</td>
<td>Recent Russian deployment of Short Range Ballistic Missiles (SRBM) including 9K720 Iskander (with a ranges assessed to be greater than 500 km) and S300 and S400 anti air systems will increasingly limit the choices available for the deployment of European forces. There is therefore a need to determine how best to defeat these systems prior to launch or, if launched, how to minimise their effectiveness so that Russian confidence in the effectiveness of these systems is reduced a level below which their utilisation would not appear to be worthwhile.</td>
<td></td>
</tr>
<tr>
<td>Areas of interest</td>
<td>Protection against SRBM including the hardening of critical assets, duplication of key sites, physical defeat including shoot down, and deception to reduce confidence that the correct targets had been selected. Defeat of very long range anti air systems including; defeat of the missiles’ terminal guidance capabilities; cyber and electronic warfare techniques to disable systems before launch and the creation of decoy and spoofing capabilities that markedly reduce adversary confidence in the effectiveness of the system.</td>
<td></td>
</tr>
<tr>
<td>Proposed approaches to research</td>
<td>Hardening of sites and creation of decoy/deception locations and activities – see the work linked to defeating the speed of enemy deployment. Area jamming, spoofing and Low Cost decoy capabilities.</td>
<td></td>
</tr>
<tr>
<td>Comment on suitability for pan-European approach and/or allocation to sub-group</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Subject | Detail | Remarks
--- | --- | ---
Initial identification of the threat/capability | Electronic Warfare (EW). |  
**Threat.** In both civil society and on the modern battlefield there is a heavy and increasing dependence on the electromagnetic spectrum for the passage of data for communications, commerce, command, control and sensor operations. Potential adversaries, including terrorist and criminal organisations, are investing heavily in their ability to control the electromagnetic environment to provide themselves with significant opportunities and advantages.  
**Response.** European societies need to identify both how they minimise their exposure to these emerging threats and how they, in turn, are able to exploit their capabilities against potential adversaries.

Initial analysis | Definition. We can define three components of EW: |  
• **Electronic Support (ES):** Surveillance of EM spectrum for immediate threat recognition and other actions such as threat avoidance, homing and targeting  
• **Electronic Attack (EA):** The use of EM to attack personnel, facilities or equipment.  
• **Electronic Protection (EP):** Protection of friendly capability against undesirable effects of employment of EW.  
ES allows the recognition of an immediate threat and its subsequent avoidance. It could be also used for homing and targeting. We should consider ELINT (Electronic Intelligence) and COMINT (Communications Intelligence) as being in this area.  
EA enables interfering with the operation of threat sensors, reducing or blocking the communication means and also confusing the opponent (to mask or hide the intention/targets by cluttering sensors). Deception could also be used by creating a false image or changing the image.  
EP reduces the effectiveness of an opponent’s ability to exploit EW by optimising own force counter-counter measures.

Areas of interest | The following areas are of R&T interest. |  
• Signal collection process (signal warning, Signal sorting and signal analysis).  
• Unwanted signal rejection.  
• Wide spectrum surveillance and Wide dynamic range (Radar long distance).  
• Jamming systems.  
• Discrepancies of signal.

Proposed approaches to research |  
• Signal separation (identification of the threat signal)  
• Data fusion (use of different sensor in order to have good situational awareness.  
• Protection of our communications/command means (radio, comms networks)  
• Protection of our surveillance means (radar, satellite)  
• Detection of the EM threat

Comment on suitability for pan-European approach and/or allocation to sub-group |  |  

<table>
<thead>
<tr>
<th>Subject</th>
<th>Detail</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Initial identification of the threat/capability</td>
<td>Countering Rapid Adversary Deployment</td>
<td></td>
</tr>
<tr>
<td>Initial analysis</td>
<td>Recent Hybrid operations have been supported by the rapid deployment of special operations forces and the deployment of conventional force to threaten or apply the use of force. European nations may not be able to rely on US satellite or other national reconnaissance assets to enable the pre-emption of the deployment of hostile or potentially-hostile forces. Research is therefore required both to improve the timely detection of the deployment of potentially hostile forces and to markedly improve the deployability of European forces to counter these hostile deployments.</td>
<td></td>
</tr>
<tr>
<td>Areas of interest</td>
<td>• Detecting the indicators of planned and actual hostile deployments including the fusion of data from social media and monitoring of a threat force’s base locations and transportation links. • Defining the optimum set of deployed equipments and logistic assets to enable the timely deployment of reaction forces. • Identifying the best means to markedly improve own forces deception and decoy activities and operations.</td>
<td></td>
</tr>
<tr>
<td>Proposed approaches to research</td>
<td>• Analysis of the key combat supplies required to generate force elements with the appropriate levels of capability to constitute a threat to an adversary requiring him to deploy greater force numbers to achieve a “guarantee” of success. • Analysis of the key infrastructure that needs to be hardened or duplicated to provide deployed European force elements with a minimum credible quantity of combat and other supplies. • Analysis of threat intelligence and electronic warfare systems to identify how best to deceive or spoof them into believing that European nations have achieved a sufficiently rapid rate of deployment to achieve deterrence. • Analysis of the optimum deployment means to enable the rapid deployment of European forces to threatened or potentially-threatened areas. This study should include the “emergency” control of the rail system to allow the priority passage of troop and equipment trains and the definition of the work required to improve the out load capabilities of essential Air, Sea and Rail Points of Arrival.</td>
<td></td>
</tr>
<tr>
<td>Comment on suitability for pan-European approach and/or allocation to sub-group</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Subject</td>
<td>Detail</td>
<td>Remarks</td>
</tr>
<tr>
<td>---------</td>
<td>--------</td>
<td>---------</td>
</tr>
<tr>
<td>Initial identification of the threat/capability</td>
<td>Big Data Attack Detection</td>
<td></td>
</tr>
<tr>
<td>Initial analysis</td>
<td><strong>Rapidly Developing Threat.</strong> In the past we have been working with the protection layer of our systems, i.e. virus protection, firewalls etc. Today, we can conclude that this is no longer sufficient. We have to look behind the protection layer and start working with prevention, get proactive instead of reactive. To achieve a positive outcome from this, we have to look at anomalies in our systems and link them together to get the whole picture of an intended/ performed attack. <strong>Increasing Societal and Economic Impact.</strong> However, in the field of hybrid warfare, it is not only our IT-systems that are under attack. Also the society and other important infrastructure are being affected. The question is what sensors we can use to find the anomalies here? How can we detect misinformation and other information campaigns when the detectors in this case are human, without creating a “big brother” society?</td>
<td></td>
</tr>
<tr>
<td>Areas of interest</td>
<td>Big Data, Social Engineering, Awareness</td>
<td></td>
</tr>
</tbody>
</table>
| Proposed approaches to research | **Detection and Sense-Making of Multiple, Conflicting and Disparate Sources.**  

- You can only understand what you can see; sensors are important, but sensors might have poor resolution (can’t see) or too much resolution (too much data). If there are things you can’t see, you can’t make judgements that support decision-making.  

- There is, therefore, a need to build an analytical model that defines a set of parameters and sensors, and their thresholds, both for systems and society. From this model it will be possible to build a methodology that detects if anomalies are connected or single activities. **Societal Cyber Education Programmes.**  

- **Meta Data.** Most people are unaware of the meta data that they generate through their use of social media. Just uploading a picture to the internet gives a lot of exploitable information, just not the picture itself, but also the meta data that describes coordinates, timestamp etc.  

- **Malware.** The most successful way to place malware or ransomware onto IT systems is through phishing emails. The feel and view of those emails are increasingly realistic; analysis by Verizon shows that 23 % of recipients open phishing mails, 11 % open attachments and about 50 % of these individuals opened the email click on links within one hour of reception. The average time to get to the first "click" is now assessed to be 86 seconds.  

- **Threat Vector.** Today’s cyber-attacks have a wide spread of methods but the weak point in any system is usually the human being and not the system itself.  

- **Education.** Research now needs to be conducted about how best to educate the population and, specially, young people in cyber protection skills. | |
<p>| Comment on suitability for pan-European approach and/or allocation to sub-group | Although this is a common threat, the diverse nature of education systems will result in national subgroupings being better able to develop and coordinate common programmes. | |</p>
<table>
<thead>
<tr>
<th>Subject</th>
<th>Detail</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Initial identification of the threat</td>
<td>ISR Technologies</td>
<td></td>
</tr>
<tr>
<td>Initial analysis</td>
<td><strong>Threat.</strong> Hybrid warfare is characterized by the coordinated use of a wide range of means, both conventional and non-conventional, and both military and civilian in nature, to achieve political outcomes. <strong>Difficulty of Detection.</strong> The use of a diverse and evolving range of means, many of them not strictly military, makes it difficult to reliably detect when a country is being the target of offensive action by another country. <strong>Response.</strong> Faced with a wide variety of possible offensive means, it is fundamental to have the ISR tools to create the broad situational awareness necessary to counter these threats.</td>
<td></td>
</tr>
</tbody>
</table>
| Areas of interest                | Focusing on the "Collect" and "Process" phases of the ISR cycle, we can identify several technology areas that may play an important role in potential hybrid conflicts. We can group those areas into two main categories:  
  - Platform related technologies, which pertain to the platforms that carry the ISR sensors;  
  - Sensor related technologies, which apply to the ISR sensors themselves.  
  In addition, there are two other domains related to ISR that will play a central role in a hybrid conflict which are covered in other research topics but are included here for completeness:  
  - Monitoring of Social Media and detection of an influence operation.  
  - Cyber awareness and defence. |         |
| Proposed approaches to research   | **Platform Related Technologies**  
  - Cooperative sensing from multiple platforms. ISR sensors on-board large platforms can be replaced by smaller and cheaper cooperative sensors on a number of platforms. In addition, these cooperative sensors can render ineffective several CC&D (Camouflage, Concealment & Deception) techniques which may be employed by the opponent in a hybrid conflict. The platforms carrying these sensors can be either manned or unmanned.  
  - Autonomy of ISR unmanned platforms. Increased levels of autonomy for Unmanned Vehicles will facilitate the execution of ISR missions, enabling these operations in highly contested or denied areas without incurring risks to personnel. In addition, these unmanned platforms will improve covert ISR collection, as UXVs are typically more difficult to detect than their manned counterparts due to their smaller size.  
  - Improving Energy Efficiency: This topic is critical for the long endurance of ISR missions. Unattended Ground Sensors with very low power consumption could operate during months providing persistent perimeter/area surveillance missions. Enhanced energy efficiency could also help to extend the time of operations of UXVs for ISR missions |         |
- **Novel Platforms for ISR collection.**
  - Airships for persistent surveillance. Airships could be effectively used for air to ground surveillance, providing exponential increases in endurance compared to fixed or rotary wings platforms, either manned or unmanned.
  - Hypersonic vehicles for ISR. Although the main interest for these vehicles relies in their capability for rapid delivery of weapon effect, hypersonic vehicles could also be employed for long range ISR of high value targets in highly contested airspace.
  - Internet of Things (IoT) - every object a potential sensor. The IoT makes possible to use objects as stand-alone sensors whose information can be collected and processed.
  - IoT Exploitation. The exploitation of IoT information might be used to detect anomalous concentrations of people which could lead to violent demonstrations or turmoil. In addition, the intelligence obtained through the analysis of the vast amount of IoT data could be critical for countering potential hybrid threats.

**Sensor Related Technologies**

- Enhanced sensors for the detection of difficult or concealed targets: Advanced ISR sensors with improved performances will play a key role in future hybrid conflicts, where concealment and deception techniques will be extensively used to try to hide that a hybrid campaign has indeed been launched.
- Detecting through cover. Through-the-wall detection technologies and millimetre and THz-wave scanning to identify potential threats inside urban areas related to hybrid campaigns.
- Detection of IEDs and UAS. For the early detection of these threats, the following sensors be needed: interferometric Synthetic Aperture Radar (SAR) for ground “change detection”, THz-wave spectroscopy for stand-off explosive detection, data fusion from different type of sensors to increase probability of detection and counter CC&D techniques, etc.

**Micro and Nanoelectronics**

- Advances in micro and nanoelectronics will help to develop ISR sensors with reduced size, weight, power and cost and increased performance.
- Reduced size and weight will allow for the integration of sensors in small platforms like micro UAV.
- Low power consumption will help to increase the endurance of ISR mission.
- New electronic materials will boost the performance of current ISR sensors, as for example Gallium Nitride (GaN) is already doing when replacing Gallium Arsenide (GaAs) in radiofrequency sensors.

<p>| Comment on suitability for pan-European approach and/or allocation to sub-group | Achieving a layered and integrated approach to ISR within Europe warrants a pan-European cooperative R&amp;T research approach. |</p>
<table>
<thead>
<tr>
<th>Subject</th>
<th>Detail</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Initial identification of the threat</td>
<td>Artificial Intelligence in the context of countering hybrid threats</td>
<td></td>
</tr>
<tr>
<td>Initial analysis</td>
<td>In order for European nations to regain the initiative it is necessary to explore and to exploit new technologies which are not currently available to military or state organizations today. One of these promising technologies is the growing sector described as Artificial Intelligence (AI). AI is the intelligence exhibited by machines/computers or software[1] that are able to act as an intelligent agent or system that perceives its environment and takes actions that maximize its chances of success.[2] Today AI technologies have become an essential part of the technology industry, carrying out much of the &quot;heavy lifting&quot; for many of the most challenging problems in computer science. AI research began in the mid-1950s; academics and students wrote programmes to solve real world problems by using algebra and developed machines' ability to communicate in English speaking. With the parallel development of more capable computers it was increasingly possible to solve more complex problems. On 11th May 1977 a computer beat the world chess champion, Garry Kasparov, the first time. For more difficult problems these algorithms, mostly based on a step by step reasoning, were faced with a &quot;combinatorial explosion&quot;: the amount of memory and computing power does not allow a step by step approach to be completed in a timely manner. The solution has been to algorithms that use intuitive judgements rather than the step by step deduction. AI is therefore a technology that is increasingly able to handle/understand/analyse the massive amount of data and information created by multiple sources including intelligence services, internet, communication channels, pictures and videos.</td>
<td></td>
</tr>
</tbody>
</table>
| Areas of interest               | Al could provide the rapid analysis to identify the initiation of hybrid conflict from amongst the clutter of the increasing proliferation of information sources including: the Internet; Global Positioning Systems (GPS); electronic devices; ground and target information; and communication technology. Two key areas identified for further research include.  
  • Natural Language Processing (NLP);  
  • Military Decision Making Process (MDMP). |         |
| Proposed approaches to research | • **NLP.** NLP gives machines the ability to read and understand the languages that humans speak and write.  
  – Very powerful NLP systems could be able to search the internet in any language to gain information, understand the content and put the relevant information together in order to provide a general operational picture.  
  – This would provide both better background information and specific alerts to decision makers and politicians. The main advantage of such machines is that they can work 24 hours a day, 7 days a week handling vast quantities of data. |         |
### Proposed approaches to research

- **MDMP.** To better deal with hybrid threats, armed forces will need to both adjust their structure and capabilities and to improve their decision-making capabilities.

  - MDMP is an iterative planning methodology that integrates the activities of the commander, staff, subordinate headquarters, and other partners to understand the situation and mission; develop and compare courses of action (CoA); decide on a course of action that best accomplishes the mission; and produce an operation plan or order for execution. MDMP helps leaders to apply thoroughness, clarity, sound judgement, logic and professional knowledge to understand situations, develop options to solve problems and reach decisions. It is a process that helps commanders, staff and others think critically and creatively while planning.[3]"

  - The agile and dynamic nature of the threat in Hybrid conflict requires military organisations to become increasingly agile and adaptive in their decision-making. Military organisations should be supported by improved information systems and computer technologies to enable them to cope with these dynamic and complex situations.

  - AI systems may be used as a supporting tool for MDMP to develop different courses of action (CoA) in a shorter time period and provide rapid analysis, evaluation and selection of competing CoAs.

  - Research will also be required to identify where increasing reliance on AI will open up new vulnerabilities and enable counter-measures to be put in place before these weaknesses are exploited by adversaries.

---

Committee 6

European Defence Cooperation and Procurement Strategies for the 21st Century: securing best value from Dual Use/Commercial off the Shelf (COTS) and/or Tailored High Tech applications

Pilots: Tuija KARANKO, Ron NULKES

Members of the Committee

Reto AMBAUEN
Marcus CATO
Amy KIMBER (Secretary)
Caroline SENZIER
Jochen SIEBENEICHER
Tero SOLANTE
Buwe VAN WIMERSMA
Franco VITTORI (Chairman)
Nikolay VELICHKOV
Yuksel YERDOGAN
Alex YERNA
Hybrid Warfare- the new threat environment and the capability needed to combat the new threat

Since 2005 following conflicts in the Lebanon and later in Ukraine politicians, military analysts and the media have pushed the concept of a seemingly new category of threat termed "Hybrid Warfare". What is being described is a shift from modern conventional force-on-force engagement in open confrontation where tactics relied on deployment of overwhelming military force and the use of "hard power" to a combination of conventional and irregular tactics which deploys conventional capability alongside disruptive technology and state troops as well as irregular formations and non-state actors. Criminal activity also plays a significant role in the Hybrid Warfare picture with terrorist attacks and crime being used to destabilise and fund operations. Many traditional militaries are finding it challenging to respond to the emerging threat picture. Aggressors have taken to using existing, readily available technology in a new way and are no longer reliant on arming themselves with traditional weapons whilst means and methods are constantly evolving and the use of insurgents, social media, cyber-attacks and below the radar criminal activity makes it difficult to pinpoint the source of the conflict and even to agree on who the perpetrators are. Moreover the instigators have little regard for the law of armed conflict, are comfortable using underhand tactics and target civilian populations as a chosen method of securing their aims.

Nevertheless, despite appearances suggesting that we are being faced with new and overwhelmingly effective form of warfare, many military strategists argue that conflicts throughout history have been defined by the exploitation of an enemy's weakness using any and all means and that warfare by its very nature is complex and multi-layered. At a recent event sponsored by NATO and organized by the Atlantic Council, attendees were told that "there is no agreed definition of terms related to hybrid warfare." In other words, the 28 members of the North Atlantic Alliance cannot agree on a clear definition of what they are facing. How can NATO leaders expect to develop an effective military strategy if they cannot define what they believe is the threat of the day? (Puyvelde, 2015). So what is really so new about Hybrid Warfare and more importantly how must we move to ensure that our defence forces are equipped with the right capabilities, in the right place and at the right time?

The West has been terrorizing itself with specters of hybrid war to an extent that it should qualify as one of history's better disinformation operations, even if it was wholly unintentional. The problem is most pronounced for European allies...Someday; we may look back on this time in Europe and call it the hybrid war scare. (Kofman, 2016)

The hybrid warfare threat and countermeasures

Hybrid warfare encompasses the full spectrum of warfare capabilities confronting the target with multiple layers of hostile actions- from undertaking subversive intelligence operations and hacking computer networks to spreading disinformation, exerting economic pressure and threatening energy supplies in an attempt to destabilise a country or an organisation. Linear "tank-to-tank" battlefields are no more, replaced instead by a wide range of more complex,
multi-layered hostile actions used to confound the opponent and achieve political objectives. Moreover, targets are no longer restricted to those that are purely military—defence personnel and infrastructure but society as a whole.

"Unlike conventional warfare, the "centre of gravity" in hybrid warfare is a target population. The adversary tries to influence influential policy-makers and key decision makers by combining kinetic operations with subversive efforts. The aggressor often resorts to clandestine actions, to avoid attribution or retribution." (Pindják)

Increasingly national defence planning has to take into consideration a threat which comprises a full range of methods including suicide attacks by highly motivated perpetrators with no regard for preserving their own lives, the utilisation of affordable readily available civilian technology, military and administrative equipment stolen and used against the original owner and cyber-attack in all its forms. Not only is the target Nation unpredictable on the grounds that terrorist attacks can happen in any country perceived to be of political importance but timing is also unpredictable and can happen anytime, anywhere.

We also have to consider the ethical dimension since it is challenging to meet the aggressors head on with like for like tactics when theirs do not adhere to the accepted "rules" of engagement. Even when public emotions are running high, especially in the wake of an attack, the reality is that we must continue to work within set legal frameworks. Recent attacks in Brussels, Paris, London, Turkey and beyond were coordinated and executed by operatives, residing within the societies they attacked, which places additional challenges on Governments trying to monitor
and prevent incidents from within their own borders. Moreover those who wage war using Hybrid techniques are often Non State or Dictatorship led and have no qualms about the use of gas, incurring collateral damage or using children and civilians as part of their strategy (Dyer). This places us immediately on a back footing since we are governed by the rules of a democratic society where public opinion decries the use of similar tactics in response. The effect on procurers cannot be underestimated since the voting public will often place limits on the type of capability they are willing to allow their Governments to use. Under the Oslo process which started in 2007 100 states including Belgium, Bulgaria, France, Germany and Switzerland signed up to the Convention on Cluster Munitions (CCM) prohibiting the use, transfer and stockpile of cluster bombs, a type of explosive weapon which scatters sub munitions (“bomblets”) over a wide area due to the severe to risk to civilians presented by their use. Though this is a clear case where there was overwhelming public support for the cease of use of a particular type of military capability it is not always the case that members of a coalition will agree on what capabilities are acceptable presenting a clear barrier to joint procurement and joint operations. And whilst it is agreed that using many of the techniques employed by terrorists as a counter attack is not the domain of a civilised society there will always be difficult decisions to made surrounding the use of non-lethal means of intelligence gathering, disinformation and so on.

In order to be able to operate in the current threat environment a hybrid adversary is likely to use a combination of advanced weapons systems alongside emerging technologies which can be used as disruptive means. So that whilst deploying hi-tech weaponry, expensive and developed over a number of years such as guided weapons they will also be looking to use readily available capability such as small unmanned air systems (UAS) for example. These UAS-low cost products, manufactured in China and available on the open market can be easily modified, require minimal training, are readily deployable and disposable. Likewise to counter the threat a combination of off-the shelf countermeasures using radar, optronics in visible and thermic spectrums installed on a tracking mount for the detection and tracking, a radio jammer, a GPS jammer or an electro-optical illuminator can be utilised to neutralise the UAS. By planning to be as adaptive and agile as the adversary we can be prepared to counter any threat used against us. Moreover, by procuring our own, more resilient UAS technologies we can stay one step ahead of the game and ensure our own situational awareness in areas that are high risk, volatile and require covert intelligence gathering.
What capability do we have?

Europe and its Allies are not completely unprepared for taking on the challenges posed by the Hybrid Warfare threat. Most countries have a level of intelligence, Special Forces, strategic communications means, some cyber warfare capability and the ability to use the media and make good use of propaganda alongside their traditional defence forces. Information sharing is a valuable and key part of European working in both the military and civilian domains. Information on crisis management is collected by NATO although this sort of evolving data is subject to obsolescence very quickly. Europe has a good track record of working at a multinational level to handle civil contingencies in circumstances where major crises impact across several National borders as we saw in the wake of flooding in central Europe, the tsunami in far east, and major industrial incidents like Chernobyl. Italy is a good example of current operations as they are currently leading a coalition of naval forces, spotting identifying and rescuing migrants.
Collaborative equipment programmes have been undertaken for years although these have not provided all the answers. A recent EU report identified some 40 capability shortfalls, of which more than a dozen are considered critical enough to have an adverse impact on the ability of European forces to deploy to theatres and to cause delays in the initial phases of an operation. (Andersson, 2015).

To maintain sovereignty and freedom of action, particularly where there are differing national interests many would argue that it is important for some defence capabilities to remain a national preserve. However in a climate of defence budget constraints it is equally important that we look for collaborative solutions which do not impact sovereignty such as exploiting mutual dependencies and engaging in collaborative programmes with those countries that share the same value and vision on Defence Security policy. And whilst it is generally agreed that there is no aspiration for the EU to own its own defence capabilities it does have the means to coordinate and support its Member States- for example via the European Defence Agency. Capability must be balanced to be effective and some countries are able to bring specific areas of expertise and equipment capability that can only strengthen our defence as a whole.

So what is needed is an inventory of Western defence and humanitarian capability to truly understand what we have in our toolbox and what can be used to formulate an effective response. It is unclear to many the full picture of bilateral and multinational arrangements that are currently in place, let alone what national capabilities could be used in a more collaborative way. The EDA are currently progressing a study to identify whether current capability action plans need to be reviewed in light of identified hybrid threats. But they remain clear that any proposals falling out of the study would be the responsibility of individual Member States to implement.

"While some progress is being made at the EU level on strategic enablers such as remotely piloted aircraft systems (RPAS), air-to-air-refuelling (AAR), satellite communications and cyber defence, the EU is now seeking to further intensify defence collaboration as a means of acquiring the necessary military capabilities to foster security in its neighbourhood and beyond" (Andersson, 2015)
What capabilities do we lack?

Europe has achieved supranational power in the fields of justice and economy, but is very far from achieving the same in the fields of security especially defence. On the one hand, member States have a tendency to cling on to their sovereignty with regards to their own defence and security forces and on the other hand can always invoke article 346 from the European Treaty to escape from applying public procurement rules when national security interests need to be preserved.

Some countries also have to cope with a background of euro-scepticism, which has a significant political impact and hinders our ability to find truly international answers to new threats. With the threat of ‘Brexit’ looming and other countries’ nationalist parties continuing to gain ground the chances of a united Europe can seem more remote than ever.

Autonomy, freedom of action and freedom of decision remain key principles of our democracies. However it could be argued that no single European country can remain insular as far as Defence and Security capabilities are concerned. Indeed, any attempt to fulfill defence and economic requirements with domestic products alone requires significant budget, knowledge and capacity beyond the realms of what is feasible. Whilst buying non-European products (namely US-products) can be time consuming and can present limitations to deployment in operational contexts.

We lack a holistic view of our defence and security capabilities, perceiving ourselves to be separate countries within Europe subject to national security interests that supersede any aspirations for cooperation and that are made up of any number of discrete national agencies working to their own agendas. Nevertheless cooperation is a fiscally appealing and practical alternative. At its most fundamental level the basis of collaboration should be a common understanding and an involvement of all European countries and their allies not limited to EU or NATO frameworks and not limited to Geographic area. It is also imperative that structures and collaborations within Government frameworks are rethought to reflect the fact that civilian targets are just as likely as military ones and to increase resilience and preparedness across all areas. Looking to existing models such as the Finnish "comprehensive defence approach" could help countries plug the gap in their ability to counter Hybrid threats.

Finland’s national defence is based on the idea of comprehensive defence approach. “Comprehensive defence approach” refers to all of the military and civil functions by which Finland’s sovereignty and the livelihood and security of its citizens are safeguarded against threats by nations and other external actors, or against other threats. Securing the vital functions of society under all circumstances with a coordinated action between different sectors of society is the key object of total defence.

(Finland, Puolustusministeriö- Ministry of Defence)
Shaping procurement to address hybrid warfare threats

So how do we equip our armed forces to address emerging threats? By establishing a short, medium and long term view of our equipment programmes, focusing on different procurement strategies (off the shelf, dual use, tailored high tech applications) and comparing national perspectives with a European Defence cooperation approach we can establish a roadmap to effective acquisition in the current climate.

How do we REACT?

In the short term- when a State is suddenly confronted it must react with available solutions within its arsenal and, where necessary buy what capability it lacks from what is readily available on the market. On being subjected to a terrorist attack, countries tend to respond by deploying heavy equipped military presence to the streets in order to secure the area whilst in parallel urgently procure supplementary capability such as GSM surveillance communications, cryptographic and tracking devices.

Western countries work within a well-defined Defence framework in order to protect their citizens and territories as well as their emergency services and their armed forces. Security policy is rooted in the use of police forces for day-to-day territorial protection with military forces for countering any external aggression against the country and its allies. The equipment capability they have tends to be designed for military and civilian use, procured via a public equipment programme and subject to rigorous regulation. Aggressors however are willing to make best use of readily available commercial technology making it very difficult to control or counter their use: standard cleaning products and high-street hardware can be used to make bombs, and any sharp implement used to carry out unpredictable attacks on the street. Likewise the proliferation of social media platforms is being used in order to carry out subversion, deception and indoctrination remotely. Access to information on the internet ensures that anyone can learn to make a bomb or carry out an attack.

So whereas conventional warfare enabled military strategists to prepare in advance for known forms of attack, monitor enemy manoeuvres and plan ahead, now detection has become increasingly difficult. And when an attack happens core programme equipment might not be the best solution for use in the highly populated urban environments that has become the battle field so that other types of equipment will be playing an increasingly important role.

✓ The two most effective procurement strategies for reacting quickly are Buying Commercial Off the Shelf (COTS) or Military Off the Shelf (MOTS) readily available solutions:
✓ COTS products or services are those that have been developed for commercial purposes, like for example IT-solutions (smartphones, computers, laptops, tablets, etc.)
✓ MOTS products are those that have been developed for military purposes and that are already available as is, such as small weapons (rifles, guns, etc.) and even some larger weapon systems which have already been developed and are in production (fighter airplane, helicopter).
When reacting to a threat or attack, if a capability gap is identified, then buying COTS/MOTS solutions offers the ability to quickly bring new equipment into service, with the only limitation being delivery lead times, clearance of export licences and for military off the shelf third party transfer agreements, which can ultimately lead to a significant delay between the expression of need (or order) and the time it can be actually used.

The disadvantage is that COTS/MOTS products are common knowledge (even to the aggressor) and that their capability is limited to the design that is being sold— they might not be tailored to the mission (e.g. smartphones without data encryption, computers services not dimensioned to react against massive cyber-attack, rifles too heavy for fighting in urban areas, attack helicopters with unsuitable weaponry).

Then there are the public procurement regulations which add layers of bureaucracy into the delivery timelines. And whilst there are exemptions which allow expedited procurement timelines for reasons of urgency (see articles 28.1.c) and 1.10 of directive 2009/81/EC) our Governments’ responsibility to adhere to legislation and protect the public purse means that procurers are bound by a certain level of regulation in all cases.

How do we PREVENT?

The medium term solution is to try and prevent attacks from occurring and at the very least have plans in place to mitigate the effect of those attacks. Information gathering and knowledge sharing amongst Western allies is the key to understanding and helping to prevent future attacks. Close cooperation with other Nations, sharing technology and committing to collaborative programmes is of utmost importance to best leverage our collective capabilities. However whilst these might seem to be the obvious solution it is no panacea and requires effort across a number of stakeholders as well as a common understanding of security, of ‘national’ / ‘supranational’ interest, common policies (export licences, transfer of technology) and security of supply throughout the member states.

One way to benefit from Industry innovation is to look at dual-use products. "Dual-use products, services and technologies can address the needs of both defence and civil communities. A large and increasing number of technologies are generic and not specific to single civil or military applications. Advanced materials, nNano electronics, information and communication technologies (ICT), unmanned systems and automation or photonics are just a few examples of fields in which research, technology development and manufacturing can be used for multiple applications. Dual-use technology transfer is the ability to adapt a technology developed in one sector (defence or civil) for use in the other (civil or defence)” (European Commission, 2014).

And we must focus not only on the attacks themselves but also on managing the aftermath: evacuation routes, handling of casualties, stabilising infrastructures, assistance to the victims, training of civilians, and control of media outlets.

Nevertheless some characteristics of hybrid warfare cannot be countered with commercially available products or services, like subversion through social media, indoctrination, destabilisation
actions (in the field of politics, media and economy), non-respect for rules of standard warfare and the Geneva Convention. In these cases we must look to direct political action, efforts in education, and diplomacy to change the tide. Only a clearly implemented joint strategy will help Europe to present a “united front” to those who seek to undermine its values. Well established agencies like the European Defence Agency should garner more support and investment to become a real defence and security solutions platform, countries should look beyond their national interest and more easily share information, ideas, technologies and capacities.

How do we PREDICT?

Aggressors are constantly improving their sophistication and abilities in virtually all aspects of their operations and support. So whilst our Intelligence Agencies never cease to stay one step ahead of those who would harm us there is no crystal ball. Nevertheless effective utilisation of a combination of High Tech applications could significantly improve our advantage and gathering intelligence will help States take action in good time.

By leveraging a group of Nations’ joint research and development capacity we can seek to grow tailored High Tech applications for the armed forces and Industry to deliver new solutions, maintain know-how, power, capability-independence, flexibility and especially the freedom to act. When tailored high tech applications are developed, it drives the whole technology of the sector and offers more possibility to act. If in Europe common Research and Development funding and execution is promoted, prediction-tools can be developed to help us counter hybrid attacks. Establishing the optimum strategy to counter hybrid attacks must also be initiated. Predicting worst cases scenarios and trying to develop solutions that could avoid those scenarios is all part of the work needed to keep us ahead of the game. This requires inputting the necessary knowledge and expertise (from both sides) and sharing it between member states to have maximum impact.

Despite this, there are numerous barriers to implementing successful joint programmes. We must question whether cooperation in the field of research and development will improve or undermine the competitiveness of the European Defence Industry as well as the ability of Europe to counter hybrid menaces on its own. Also research and development programmes can be long and expensive. It requires an on-going commitment by governments to see them through and support them over the long term with sufficient political will and resources.
How do we fund capabilities?

The answer might be "primarily nationally". Nations have the ability to develop defence and security systems able to meet emerging threats, but this usually demands an increase in defence expenditure and remains a political choice.

By increasing bilateral and multinational cooperation it should be possible to get "more bang for the buck". Neighbouring countries and political allies should explore all the possibilities to combine purchasing power and reduce duplication of effort in order to keep their security systems interoperable and effective.

In the last 20-30 years numerous attempts to collaborate bilaterally and multinationally in the defence and security field have been conducted in order to exploit mutual dependencies and strengthen the might of the European defence Industrial base withbase with varying results. The Letter of Intent on Measures to facilitate the Restructuring of the European Defence Industry (2000), ratified by 6 Defence Ministers (France, Germany, UK, Italy, Spain and Sweden), is one such example. It aimed to identify areas in which the participants could work to establish common solutions to common defence problems. By defining the common principles, organisations and responsibilities it aimed to negotiate appropriate follow-on arrangements and agreements that could lead to the amendment of national regulations where appropriate. In doing so the Participants have accepted 'mutual interdependence and the possibility of abandoning industrial capacity' for the benefit of a company located within the territory of another Participating State. Success could be perceived to be limited but one successful programme conducted under the Letter of Intent (LoI) framework is the European missile programme BVRAAM (Beyond Visual
Range Air to Air Missile) which delivered the Meteor missile that will be operational – for the first time – on the SAAB Gripen C/D MS20 with the Swedish Air Force during the second quarter of 2016. However the political, industrial and military landscape has changed significantly since the LoI signature: the EDA was established in 2004, the European Commission has taken an ever closer interest in defence industrial and market issues and the defence industrial base has become increasingly globalised. (UK Government, 2012) The Lancaster House Treaties (2010) are two treaties established between the United Kingdom and France to improve defence improvement defence and security cooperation. Building on commitments made in the UK Defence and Security review to strengthen ties between the two European allies with closely matched security interests and capabilities the treaties sought to significantly ramp up bi-lateral cooperation in a number of areas. Aspirations included the sharing and pooling materials and equipment, encouraging mutual access to each other’s defence markets, collaborating on the technology associated with nuclear stockpile stewardship in support of both countries’ independent nuclear deterrent capabilities and the construction of joint research facilities in both countries. An LoI was also signed to create a new framework for exchanges between UK and French Armed Forces on operational matters. In an Industrial context the UK-France High Level Working Group was directed to strengthen its work on industrial and armament cooperation leading to the creation of Centres of Excellences on identified industrial capabilities thereby ensuring a mutual co-dependence. Major joint missile programmes have also been launched to provide substance to the establishment of such Centres of Excellences. (UK Government, 2015)

This type of bilateral cooperation on acquisition purchase, development of joint military doctrine and training programmes, alignment of logistical requirements and mutual access to Defence markets seeks to leverage benefit from pooling resources whilst also maintaining freedom of decision over where each Nation’s troops are deployed.

Funding for research is one area which struggles to compete in a climate of decreasing defence budgets. Years of under investment in defence research is being cited as one of the main barriers in the way to allowing the EU to realise its members and allies’ ambitions for it to become a true "Security Provider". Political Bodies are now beginning to react and the European Parliament launched an initiative in 2014, which has since gained considerable momentum and support from the highest political level, known as the EU Preparatory Action (PA) on defence research. The PA is a flexible tool outside Horizon 2020, the EU’s largest Research and Innovation programme. Horizon 2020 itself includes dual-use and security research activities, but no defence research. The PA will run over a three year period (2017-2020) and test, on a small scale (maximum €100 million), the feasibility of a fully-fledged EU defence research programme, which could then lead to a major funding allocation (possibly in excess of €3bn) in the next Multi-annual Financial Framework (MFF 2021-2027). (ASD, 2016)

(12) European defence research as a whole has declined sharply since 2006. Between 2006 and 2013, EDA countries’ Research and Development has been reduced by a staggering 29.2 %, from EUR 9.7 billion (EUR 10.6 billion at constant price) to EUR 7.8, and Research and Technology by 27.7 % from EUR 2.4 billion (EUR 2.9 billion at constant prices) to EUR 2.1 billion. Defence R&D has decreased at twice the rate of defence expenditure (14.7%) and is thus the main victim of budget cuts.) (European Parliament, 2016)
Finally, by increasing the role of EU institutions and international agencies in financing and procurement, Europe could leverage its ability to counter any hybrid menace. One proposal is for the EU to establish a common funding for defence and security or for one agency to manage the acquisition process when common requirements are established. And by increasing cooperation to other areas of homeland security and emergency response we can hope to establish further avenues for economies of scale and common doctrine.

Figure 3 Defence Budgets Continue to Fall in the West (Jane’s Defence Weekly)
Role of industry

Industry has always had a key role in developing the right capabilities on behalf of defence and security forces. Closer working between industry and defence can only strengthen our ability to respond to current security challenges in our region. But often political and economic interests can hamper the partnership. Moreover, the legal framework is not always conducive to close working between Industry and Defence customers where competition is the bedrock of the acquisition process. As the Netherlands Commissariat for Military Production has succinctly described: the defence materiel market is not a level playing field. Many countries prefer to purchase military systems from their own national defence industry. Foreign suppliers are therefore less likely to be awarded contracts (Government of the Netherlands).

By doggedly pursuing domestic defence contracts are we not limiting our ability to secure the best capability there is on the market? Can we not maintain a secure and competitive Industrial Base in our own country on the one hand, whilst also making the best of an International competitive market on the other- do they have to be mutually exclusive?

The key objective of the European Commission’s defence industrial policy is to develop a competitive and innovative European Defence Technological and Industrial Base (EDTIB). An EDTIB is important for an effective EU Common Security and Defence Policy (CSDP). This policy is designed to provide the EU with the capacity for autonomous action when responding to international crises, without prejudice to actions by NATO. (European Commission, 2016)

It is important to keep pace with emerging technology developments as well as to harness much of the innovative thinking happening within Small to Medium Enterprises (SMEs) who have a level of flexibility not afforded to larger Defence Industry players. For example the French RAPID (Régime d’APPui à l’Innovation Duale) is a French initiative lead by Direction générale de l’armement (DGA) whereby SMEs can submit innovative projects, with the financial and organisational backing of a large company. The project is designed to be fast moving and allows many projects to begin just a few months from submission of the proposal. For relatively little investment (most projects are up to 1M€) it is hoped that Defence will be able to secure a high level of innovation from a wide pool of expertise.

We should also be looking to Industry to help us develop key capability targeted for use across a wide number of end users and multiple nations. Utilising the market to develop multi-agency and cross border process and procedures as well as data handling we can improve our "message and means" capability. For example TETRA TErrestrial Trunked RAdio (TETRA) is a radio communications system which was specifically designed for use by government agencies, emergency services, public safety networks, rail transport staff and the military. It is now widely used for cross border communication between Norway and Sweden.
Conclusion

The Hybrid Warfare scare. The Term "Hybrid Warfare"- coined in 2005 and for which there is no agreed definition suggests that there is something new about the way modern warfare is waged. This is far from the case since while conflicts are reaching wider into the Cyber domain and terrorism is the top of everyone’s agenda there is nothing particularly novel about using a combination of warfare tactics to gain superiority. So whilst the term may have its uses as a conversational short form, Defence policy makers instead need to be focusing their attention on the complex portfolio of specific interrelated threats that we are faced with and the capability needed to address those threats.

In practice, any threat can be hybrid as long as it is not limited to a single form and dimension of warfare. When any threat or use of force is defined as hybrid, the term loses its value and causes confusion instead of clarifying the "reality" of modern warfare.  
(Puyvelde, 2015)

Civil Military Resilience. We must look to increase resilience and preparedness in our territories by investing in civil military contingency planning and capability. When defence augments civil capacity we increase the likelihood of success in managing crises and restoring stability. Information sharing, joint training, enforcing the preparedness of civil resources such as railways, ports, airfields, airspace and infrastructure, collaborative procurement and effective legal frameworks can only lead to a more effective "collective defence" model.

Allies need to adapt constantly as new vulnerabilities and threats emerge from non-state actors such as so-called Islamic State, as much as from state actors like Russia. Resilience is here to stay as a core element of collective defence.  
(Shea)

Procurement Responsibilities. We must devise effective procurement strategies which secure best value for money solutions to our capability needs by targeting COTS and MOTS commercially available solutions in the short term to counter immediate threats, commit to a sustained programme of collaborative defence programmes to strengthen collective capability and make best use of research opportunities to develop hi-tech, innovative solutions to modern challenges in the cyber domain. It is no longer enough to procure equipment and hope for the best. We must be looking for opportunities to deploy what we have in new ways, leverage innovation from Industry and pool our resources.

Effective procurement and support of defence equipment is not a “nice to have”, but an essential part of maintaining flexible, battle-winning Armed Forces.  
(UK Secretary of State for Defence, 2013)

Collaborative working is key. Only European developed and owned capabilities can provide the necessary freedom of action and decision whilst igniting the operational and industrial power that we have on our doorstep. Information sharing, bi-lateral and multinational collaborative
programmes, joint exercises, reciprocal research efforts, and critically, a dedicated push to improve interoperability will enable us to make the most of our depleted defence budgets and to maintain our strategic autonomy. Capitalising on what each Nation can bring to the party and presenting a united front is the best way to ensure that we can secure sufficient capability to survive in an increasingly unpredictable defence and security environment.

"Even the strongest soft powers cannot make do in the long run without at least some integrated defence capacities; integrated defence capacities, more synergies in defence procurement and permanent structured cooperation is the way forward."

(Juncker, 2014)

Where do we go from here?

What is clear is that without the political will and high level leadership to engage wholeheartedly across national boundaries and to make best use of the full suite of existing capability and political instruments that we have in our toolbox we are unlikely to succeed in our defence and security ambitions. There is a risk that we rest on our laurels, seeking comfort in the fact that we reside in the West and continue with nothing more than a few very public statements of good will. What is needed is a step change in our defence and security thinking to end un-coordinated and isolationist military planning. Only then can we achieve our foreign policy goals and have the autonomy to effectively address the issue of security in the current climate in order to achieve a safe, secure and prosperous Europe.

Free riding in defence and security has come to an end. ..The security environment necessitates that European defence stops being a "paper tiger" and becomes a fully-fledged policy providing equal security and equal concern for vital security preoccupations for all…This will require strong leadership to overcome the political deadlock. We do not need to invent new heavy or complex structures, mechanisms or tools. Those that already exist need to become an operational reality (EPP Group, 2016)
Main references


Pindják, P. (n.d.). NATO REVIEW: Deterring hybrid warfare: a chance for NATO and the EU to work together?


