Finabel

Focused Question

Emerging threats and challenges of the EU Land Forces

AN EXPERTISE FORUM CONTRIBUTING TO EUROPEAN ARMIES INTEROPERABILITY SINCE 1953

FINABEL
European Army Interoperability Center

This focused question is a document that gives an initial reflection on the Finabel annual theme 2018-2019. The content is not reflecting the positions of the member states, but consists of elements that can initiate and feed the discussions and analyses in the domain of the theme. It was drafted by the Permanent Secretariat and is supported by the organization.

Today's world is rapidly changing. The European neighbourhood has become increasingly unstable during the last 20 years: new opportunities, new practices and new threats have emerged since the end of the Cold War. The digital era has brought opportunities but also raised concerns for our security. IT has increased the volume of available and useful data but paradoxically has made them more vulnerable. Security is an ever-evolving process. That is why it is essential for European states to stay aware and adapt to the opportunities, threats or challenges that shape our future. In this process, the military has a role too. In this food for thought paper, Finabel identifies three challenges and threats European land forces face today – and will increasingly face in the future – and shares reflections to address them.

CHALLENGE NO 1: DIGITAL TECHNOLOGIES

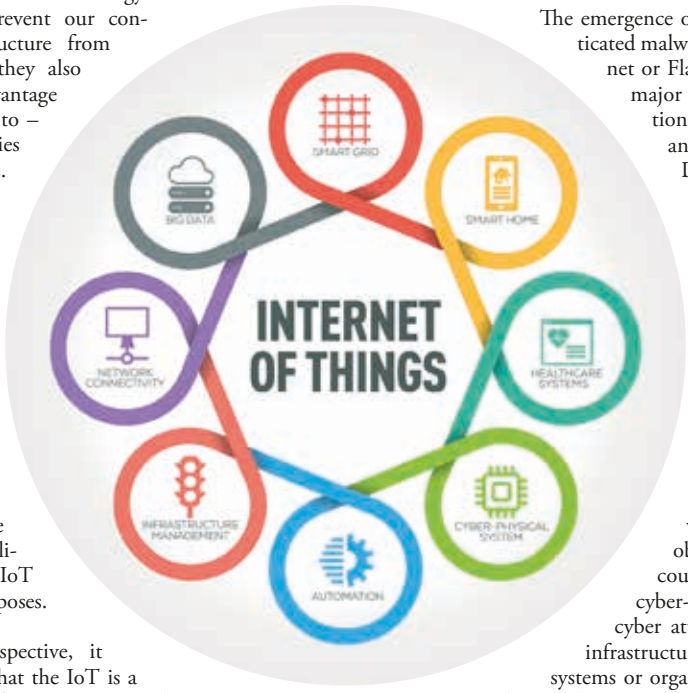
In the past decade, the world has experienced the development of information and communication technologies into all aspects of life. From a military perspective, three developing fields deserve all attention: internet of things, cyber security and artificial intelligence.

Internet of things (IoT)

More and more devices are connected to the internet and remotely operable. It ranges from the coffee machine and the refrigerator to surveillance and attacks by drones. This technology represents at the same time concrete opportunities (time and efforts savings) and increased vulnerability.

In its 2015 *Digital Single Market Strategy*, the European Commission has emphasised the possibilities of the Internet of things (IoT). A growing number of devices is connected to the internet and infrastructure as well as vehicles are planned to be connected after the 5G network will make its introduction in Europe. If not secured, interconnectivity of all devices, even the ones of our daily activities, may constitute a threat and give rise to a new form of terrorism: the hacking and takeover of connected devices. For instance, autonomous cars could be hacked and steered towards the roadside or maneuvered into any other dangerous

situation. A disruption of the internet, for instance by cutting transatlantic cables, could cause massive shutdowns that would render a country powerless and would cost billions to targeted economies. If states must develop this technology with caution and prevent our connected infrastructure from cyber attacks, they also should take advantage of – and adapt to – the opportunities IoT constitutes. Share intelligence on real time, directly connect decision-takers to the battlefield, control devices from remote location, direct weapons on identified targets could be some of the applications of the IoT for military purposes.



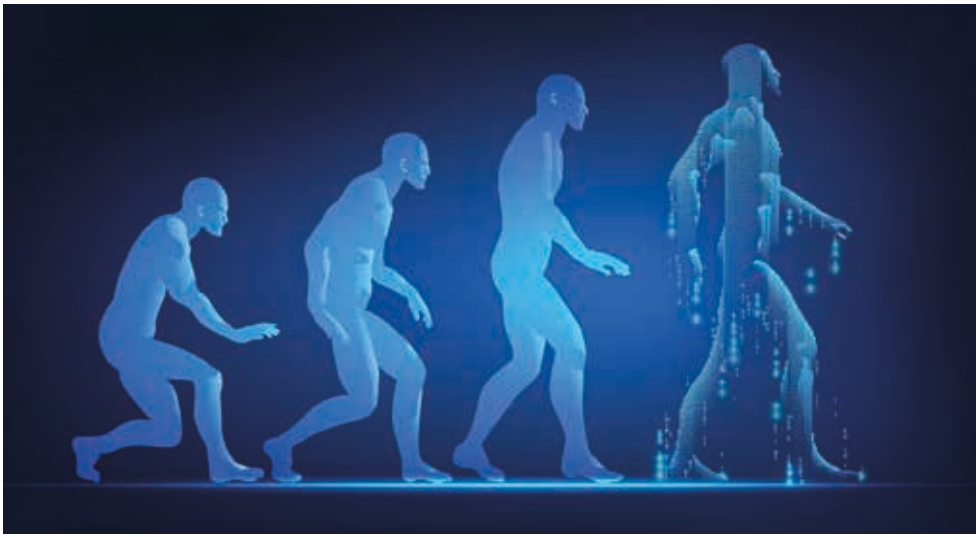
From this perspective, it becomes clear that the IoT is a major concern for our security. The success of conventional land forces operations is currently enabled by, and dependent on the assured availability of, and access to, cyberspace. In this new context, EU land forces can be threatened by cyber attacks either in wartime, periods of low-intensity conflicts or peacetime.

Cybersecurity

Cyberspace is recognised as the 5th operational domain besides land, sea, air and space. Everyday, states and non-state actors are launching cyber attacks against state departments and private companies. These attacks have various purposes: pranks, theft of information or money, spying, disinformation, destabilisation, display of force, assessment of cyber defence, etc. Cyber threats have become ubiquitous, increasing in scope and more sophisticated for both civilians and militaries. The low cost, high-potential impact and general lack of transparency of these cyber attacks make them attractive for both powerful and less powerful actors.

The emergence of highly sophisticated malware such as Stuxnet or Flame represents a major shift from traditional mass phishing and Distributed Denial of Service (DDoS) cyber attacks towards Advanced Persistent Threats (APTs). APT refers to a long-term pattern of highly developed hacking attacks, with a clear objective, which could range from cyber-espionage to cyber attacks on critical infrastructures, operating systems or organisations, usually aimed at governments by well-resourced state actors, or agents affiliated with states. The threat here is that while passive cyber defence measures can prevent low-level attacks, it is no longer the case in countering complex cyber attacks as "Advanced Persistent Threats". Indeed, through intelligence gathering analysis, they are able to target system vulnerabilities or behaviour and can easily circumvent existing network defences.

Not only military infrastructure is targeted but also civilian infrastructure is at risk. In 2016 a Ukrainian power plant was hacked for several hours with a power outage as result. Specialists speculated this attack was just a reconnaissance of Russian hackers in preparation of a possible large-scale assault. In Ukraine it took hours to switch the powerplant to function manually. In war time the absence of power and solid communication would be considerably dangerous as there is a considerably large dependence



on civilian communication in peace time. Combined with a physical invasion, such a cyber attack could be devastating.

Artificial intelligence (AI)

Artificial intelligence (AI) is the ability of a technical device to carry out tasks autonomously, learn from previous experience and develop its own alternative solutions. Further development of AI is about to have influence on both military- and civilian digital infrastructure. This technology has passed the first stage of research and is already in development – and in some sectors quite advanced. In 2016, the Defence Advanced Research Projects Agency (DARPA) from the US, organised a competition in which companies had developed AI software used to carry out hacking assaults on computers with similar software. The hacking software was able to adjust its approach by finding weak spots in the computer system and kept a continuous flow of attacks aimed at the target computer. Improved versions of similar software would be able to learn quickly and send out continuous and numerous waves of hacks aimed at digital infrastructure. To adapt to these threats, standard operating procedures with counter measures and guidelines on how to switch to a manual system should be developed and applied in order to be prepared in the contemporary age.

AI could rewrite the way militaries operate and cooperate entirely, whether it be in logistics or warfighting. AI should obviously be seen as a useful tool, but it is also a prominent modern threat. AI has several applications such as data management or algorithms anticipating the enemy's movement. Some could potentially save lives or limit casualties: localising mines and IEDs in the field via intelligent vehicles, decision support through the use of data and surveillance tasks via unmanned vehicles. AI in cyber security can be used both for offensive and defensive purposes. On the defensive side, human IT security administrators need to know what is happening on the networks to scope the severity level of attacks, assess possible consequences and draft potential countermeasures. AI systems can detect between 80% and 90% of attacks and they can review billions of lines of data logs each day, a number not achievable by humans; this could help assess and improve risk analysis and could prevent inefficient expenses. However, the military cannot rely entirely on AI yet. *"Robots do not have the experience, the knowledge, the emotions, the passions and everything the humans have"* the Pentagon concludes.

However, even if AI is an outstanding asset for militaries, it can also be a high-level threat, especially when it comes to "robot fighters". Machines could increase violence on the battlefield, and evade human control. If spread in western armies, they might also fall into

the hands of enemies or terrorist groups in the years to come. The main issue would be to deal with unconventional – and widely unpredictable – weapons that are not remotely controlled but autonomous and self-improving.

CHALLENGE NO 2: DISINFORMATION

Another challenge is disinformation, information that is intentionally false, and misinformation, information that is unintentionally false. Even if propaganda and subversion is not a new phenomenon as such, the development of communication technologies has changed the way (dis)information is produced and disseminated. While traditional propaganda is a state tool that exacerbates specific emotions of a public to induce an expected behaviour (vote, conscription, engagement), disinformation today is less straightforward and mixes facts, exaggerations or rumours to produce rational but false interpretation and conclusions and transmit them along with true information. In this respect, the internet and social networks constitute perfect channels for easy, large, fast and targeted dissemination of information with few traceability.

The last year has shown the important impact fake news and web trolls could have on electoral results. Same processes are also at work on battlefields against military personnel or civilians in conflict areas. Where forces face each other, fake or targeted information can be spread to discredit the enemy, discourage its soldiers and exert pressure (stress, scare, humiliate, threaten) on populations hosting them.

Here below, three recent examples illustrate how fake or targeted information has been used to destabilise enemy's military. A striking illustration of information warfare is Ukraine which has become the ground of permanent disinformation attacks from both sides of the current conflict, accusing each other of violation of ceasefires, border incidents or subversion. A pro-Russian group of hacktivists, called *CyberBerkut*, is regularly hacking government's, defence ministry's as well as NATO's websites and correspondence to reveal military strategic machinations. The danger of these claims is that they cannot be proven, denied or refuted easily and that they leave the Ukrainian government powerless. Recent NATO joint exercises in Baltic republics (Enhanced Forward Presence) have also been subject to disinformation. In Latvia, Canadian forces have been *"the target of repeated information-warfare salvos in the five months since they arrived in the tiny Baltic country, as fake news designed*

to discredit NATO forces is routinely disseminated online". Rumours that are disseminated imply the accomodation of troops in luxury apartments at taxpayers' expenses, enriched with pictures of American soldiers drinking beer in a Latvian bar or military rations discarded in the woods. The objective is clearly meant to discredit Canadian troops and NATO in the eyes of the hosting population. One last example concerns the last Zapad exercise, a military joint simulation of Russian and Belarusian troops launched in November 2017 on their Western border. Before its deployment, NATO analysts and officials were estimating the number of troops involved to 100.000. However, according to Belarusian authorities the exercice only involved 12.700 men. This huge appraisal gap demonstrates how misinformed NATO has been on Russia's intent. The increasing use of information-warfare, mostly from Russia, cannot be underestimated. Although moral considerations prevent the development of offensive disinformation, European armies should develop defensive tools to react to such attacks at home and abroad where troops are engaged.

CHALLENGE NO 3: POLITICAL WILL AND MILITARY INTEROPERABILITY

With no surprise, the dispersion and the disparity of forces within the EU remains a significant barrier to military efficiency. Although the treaties of the Union advocate for more cooperation since the Treaty of Maastricht, integration of defence policies remain a very sensitive topic.

Member states should shape the European defence policy once and for all, establishing strategic priorities, create rules for procurement, avoid redundancy, ease decision-making, etc. Of course, progresses have already been achieved in this direction: a EU military staff (EUMS) and committee (EUMC), European Defence Agency (EDA), the permanent structured cooperation (PESCO), the European Security Strategy (ESS), EU Defence Funds (EDF), multinational industrial projects, EU battlegroups (EUBG), etc. but they remain voluntary and defence policies remain linked to national sovereignty. However, since today's threats are the same for all member states (Russia's expansionism, terrorism, nuclear proliferation, natural disasters, mass migration, …), there are few arguments in favour of distinct defence policies. Possibly the idea that interoperability between European forces could lead to a European Army has discouraged capitals to lose their sovereignty.

Besides top-down efforts for integration, the military can also foster a bottom-up impulse. Projects that member states have agreed on under the PESCO agreement could be a starting point for more technical progresses in terms of defence within the EU. The years to come will show the citizens whether the European Union is ready and capable to face the threats that are already upon us and the ones which are about to come.

SUGGESTIONS & CONCLUSION

This paper depicts the main concerns and opportunities our land forces will have to deal with in the near future. The use of IoT, cyber space and AI gives thought for concerns on the vulnerability but also the opportunities of increased automatisation. AI can both be used in software and hardware and the capabilities of both systems should be explored to determine what it can offer the European armed forces. New technologies also provide ideal channels for disinformation dissemination, from which states should prevent. Finally, the dispersion of European forces hugely contributes to the weakness on the continent. The reserved attitudes of member states regarding incorporation of European defence facets is not contributing to more European military interoperability as it is within a voluntary framework. Decision-makers but also military officials are responsible for achieving greater cooperation and synergies in the military field.

In practice, several actions could be undertaken to adapt our societies to the changes in our environment and prepare our defences to emerging threats.

- Share practices and experience through specific hubs or centres of excellence (for example a EDA research programme) without hiding all documents behind a secured environment;
- Allow/oblige the transfer of breaching data from civilian and military entities to improve R&D;
- Develop/support the high-tech sector, namely in cyber security, IA and IoT;
- Build cyber defence capabilities with EU Member States (MS);
- Build the EU Cyber Defence Policy framework;
- Promote cooperation and share expertise between the private, public and military sector;
- Raise awareness on disinformation and encourage MS to prevent it;
- Downgrade the security level of lessons learned documents to increase the distribution of these documents for exploitation at all levels;
- Create bottom-up interoperability, evolve from bilateral to multilateral approach.

BIBLIOGRAPHY

- Blackwell T., Russian fake news campaign against Canadian troops in Latvia, The National Post, November 2017. Consulted on 20 March 2018, from http://nationalpost.com/news/canada/russian-fake-news-campaign-against-canadian-troops-in-latvia-includes-propaganda-about-litter-luxury-apartments
- Elazari, K. (2017). *Hackers are on the brink of launching a wave of AI attacks*. Consulted on 27 March 2018, from http://www.wired.co.uk/article/hackers-ai-cyberattack-offensive
- European Commission. (2016). *Digital Single Market.* Consulted on 27 March 2018, from https://ec.europa.eu/commission/priorities/digital-single-market/
- Haines J. R., *RUSSIA'S USE OF DISINFORMATION IN THE UKRAINE CONFLICT,* Foreign Policy Research Institute, February 2015.
- Röhrig, W. & Smeaton R., *CYBER SECURITY AND CYBER DEFENCE IN THE EUROPEAN UNION OPPORTUNITIES, SYNERGIES AND CHALLENGES*. Consulted on 27 March 2018, from https://www.eda.europa.eu/docs/default-source/documents/23-27-wolfgang-r%C3%B6hrig-and-j-p-r-smeaton-article.pdf
- Vallance, C. (2016). *Ukraine Cyber-Attacks "Could happen to UK"*. Consulted on 27 March 2018, from http://www.bbc.com/news/technology-35686493
- Wong A., Eng C., Loh Ming Yao R. & Ng. J.. *Cyber Threats in Hybrid Warfare: Securing the Cyber Space for the RSAF.* Consulted on 27 March 2018, from https://www.mindef.gov.sg/oms/safti/pointer/documents/pdf/V43N1a3.pdf

Created in 1953, the Finabel committee is the oldest military organisation for cooperation between European Armies: it was conceived as a forum for reflections, exchange studies, and proposals on common interest topics for the future of its members. Finabel, the only organisation at this level, strives at:

- Promoting interoperability and cooperation of armies, while seeking to bring together concepts, doctrines and procedures;
- Contributing to a common European understanding of land defence issues. Finabel focuses on doctrines, trainings, and the joint environment.

Finabel aims to be a multinational-, independent-, and apolitical actor for the European Armies of the EU Member States. The Finabel informal forum is based on consensus and equality of member states. Finabel favours fruitful contact among member states' officers and Chiefs of Staff in a spirit of open and mutual understanding via annual meetings.

Finabel contributes to reinforce interoperability among its member states in the framework of the North Atlantic Treaty Organisation (NATO), the EU, and ad hoc coalition; Finabel neither competes nor duplicates NATO or EU military structures but contributes to these organisations in its unique way. Initially focused on cooperation in armament's programmes, Finabel quickly shifted to the harmonisation of land doctrines. Consequently, before hoping to reach a shared capability approach and common equipment, a shared vision of force-engagement on the terrain should be obtained.

In the current setting, Finabel allows its member states to form Expert Task Groups for situations that require short-term solutions. In addition, Finabel is also a think tank that elaborates on current events concerning the operations of the land forces and provides comments by creating "Food for Thought papers" to address the topics. Finabel studies and Food for Thoughts are recommendations freely applied by its member, whose aim is to facilitate interoperability and improve the daily tasks of preparation, training, exercises, and engagement.

FINABEL
Quartier Reine Elisabeth
Rue d'Evere 1
B-1140 BRUSSELS

Tel: +32 (0)2 441 79 38
GSM: +32 (0)483 712 193
E-mail: info@finabel.org

You will find our studies at
www.finabel.org

Responsible publisher: Mario BLOKKEN - Finabel Permanent Secretariat - QRE - Rue d'Evere,1 - B-1140 Brussels - +32 (0)2 441 79 38