Finabel

Finabel Study

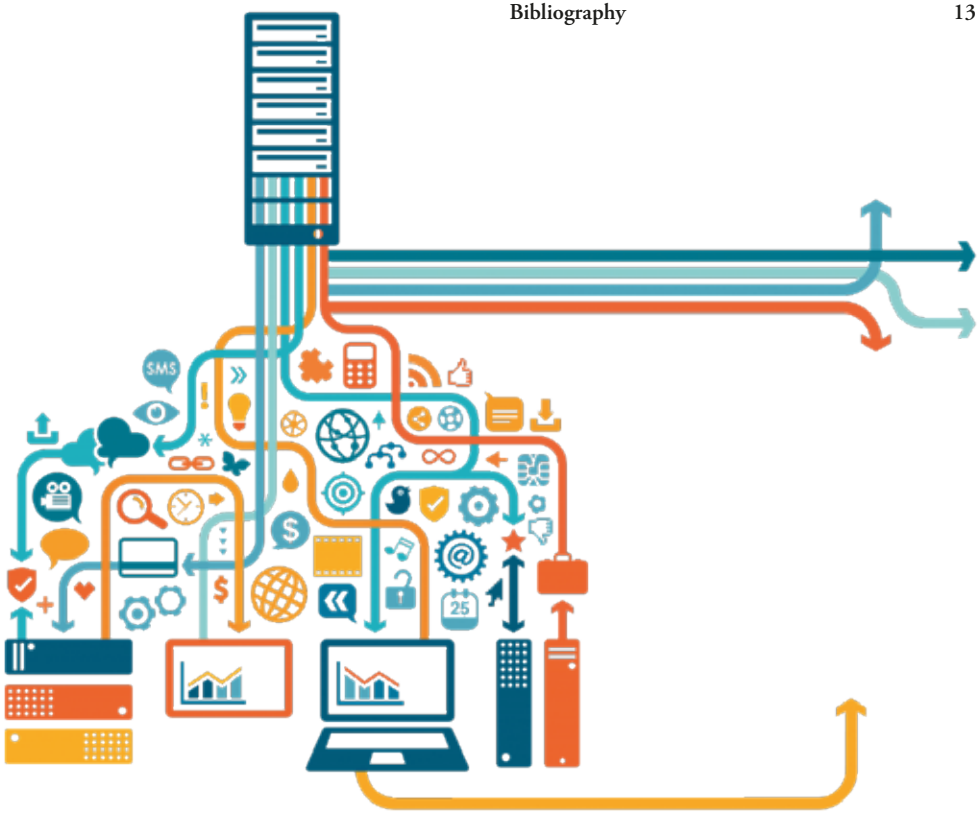
Data manipulation: The cyberthreat of future military operations

AN EXPERTISE FORUM CONTRIBUTING TO EUROPEAN ARMIES INTEROPERABILITY SINCE 1953

FINABEL
European Army Interoperability Center

This text was drawn up with the help of **Mr Fabien Galle**, trainee, under the supervision of the Permanent Secretariat.

TABLE OF CONTENT



INTRODUCTION

Westphalian vision of international relations is pregnant in the way States consider their cyber arsenal: domestic interest and sovereignty reign to insure their equality on the globe. Just to remind that balance of power proved its limits when total war arises from power confrontation. Whereas cyber weapons are disruptive due to attribution endeavor[1], their spreading potential, while they are sweet to public but harmful to targets, represent « threats to the peace » in respect to the interpretation of the first Article of the UN Charter, first paragraph, because they can be considered as an act of agression. But in many cases, conflicts in the cyber space will not reach that point of no return, because when a breach is detected, it is hard to identify its provenance. We could compare the cyber weaponry to the one of a guerrilla: its position known, its force is reduced to void. Yet it is inconceivable that with only a few fiber optic transatlantic cables routing all the internet traffic, owned by major IT companies, this identification is still driven impossible to resolve. Technically, it makes a long time ago that those networks are being scrutinised by some foreign intelligence agencies, but the core issue is the amount of data collected as they are not targeted and the filtering process is manually impossible and automatically not sufficient.

Can we count on artificial intelligence to be the silver bullet? What are the legal and economical implications of a global eavesdropping? Are we prepared to thwart a massive attack on our vital infrastructures, from where will it comes from, and what strategies can we put in place to avoid that catastrophic scenario? Such questions raise many others about the limits of our confidence in technological advance to safeguard our privacy and secure our numeric well-being. Our duty resides not only in our capacity to consider what future threat might consist of, but in our current open mind abilities to build a resilient system architecture at the scale of the European territory we have to protect. This ambitious project depends on political views to reconcile: can we trust our allies if their offensive power allows them to enter or shut down our cyber structure too easily?

Incidentally, manipulation is by definition a technique of defence, used by a subject to influence others without their knowledge, or the fact of counterfeiting reality. Whilst it is more sensible to expose the exponential surge of data treatment by IT corporations: over 24 petabytes everyday[2]. Taking up the challenge of big data is not just about their treatment, it requires competencies and prioritisation, in a world of scarce human resource management and machine deep learning competition. The impact of this civil - military evolution on a battlefield that moves dangerously into the heart of the city and in the mist of the cloud is as disturbing as the electronic waves it comes from. To avoid the engulfing, here is some anchor in the rough sea of 2020 30B IoT cyberworld.

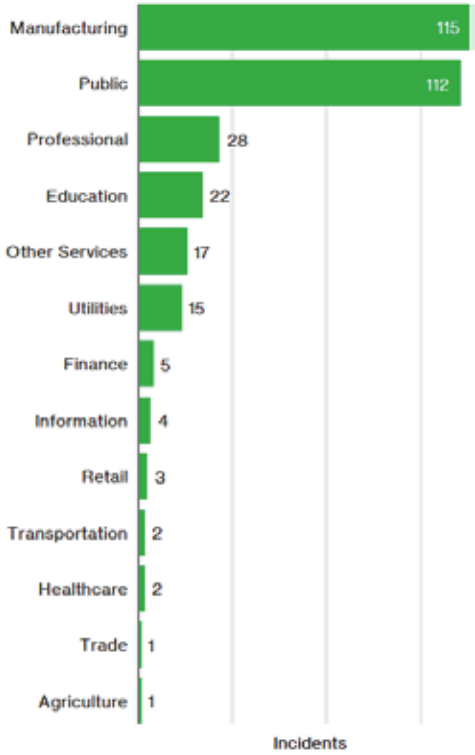
[1] Limnéll Jarno, « Proportional Response to Cyberattacks », *Cyber, Intelligence, and Security*, June 2017, p. 38.
[2] Schönberger Viktor Mayer & Cukier Kenneth, *Big Data, La révolution des données en est marche*, Robert Laffont, 2014, p. 17.

AN AUTONOMOUS WARFARE DOMAIN

Cyberspace is an emergent domain[3]: the fifth theatre of operations after earth, sea, air an space[4]; with a shift operating to urban conflicts (comparable to terrorism)[5]. When the use of electromagnetic fields proliferate as a cheap mean to experiment resistance of network or neutralise even offline target, that let think a cyber-Pearl Harbor scenario is still possible up to now[6]. Whereas drone era and Internet of Things (IoT) brings more furtive and potentially disruptive physical entry points.

Manipulation of data is assimilated to vandalism instead of warfare by some scholars, while others compare cyber attacks to ballistic ones[7]. This analogy has the interest of simplifying the scope of this new field of study, but has the weakness of minimizing its potential contagious effects. Recent WannaCry ransomware pandemia illustrates how an initial tool preserved for surveillance issues by the NSA can turn vinegar[8] in cyberspace. Maybe it is the reason why NATO has consecrated it an independent warfare arena[9]?

In cyberspace, « companies becomes as much issues than actors and State is considering this new situation, searching to associate them to his combat in this modern and irregular war[10] », even more challenging than terrorism[11].



Count and percentage of breaches within Cyber-Espionage (n=271). « Verizon 2017 Data Breach Investigations Report », *Verizon*, 27th April 2017, 10th Ed, http://www.verizonenterprise.com/resources/reports/rp_DBIR_2017_Report_en_xg.pdf, p. 42.

[3] Establier Alain, « La sécurité numérique par ceux qui la conçoivent et la pratiquent », *Sécurité globale, ESKA*, 2016/4, p. 32-44; Limnéll Jarno, « Proportional Response to Cyberattacks », *op. cit.*, p. 37-40.

[4] Muller Feuga Philippe, « Cyberespace, nouvelles menaces et nouvelles vulnérabilités », *Securité globale*, ESKA, 2017/1, p. 84.

[5] Establier Alain, « La sécurité numérique par ceux qui la conçoivent et la pratiquent », *op. cit.*, p. 15-45.

[6] Muller Feuga Philippe, « Cyberespace, nouvelles menaces et nouvelles vulnérabilités », *op. cit.*, p. 93-94; Raufer Xavier, « De la cyber-jungle au cybermonde », *Sécurité globale, ESKA*, 2016/4, p. 6; Delesse Claude, « La NSA, «mauvais génie» du cybermonde ? », *Sécurité globale*, ESKA, 2016/4, n°8, p. 85.

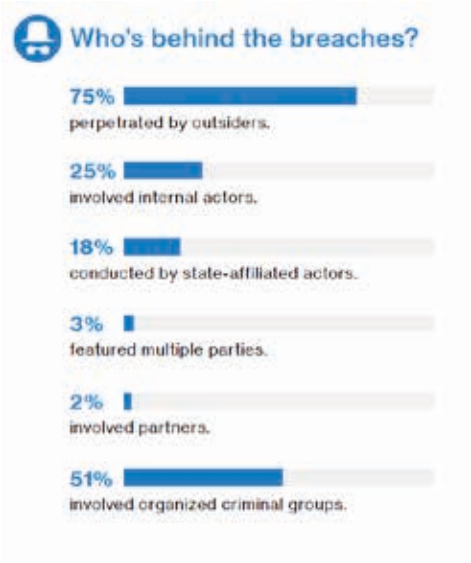
[7] Sternberg David, « Framing the Cyberthreat through the Terror-Ballistics Analogy », *Cyber, Intelligence, and Security*, June 2017, p. 128.

[8] Sherr Ian, « WannaCry ransomware: Everything you need to know », *Cnet,* 19th May 2017, https://www.cnet.com/news/wannacry-wannacrypt-uiwix-ransomware-everything-you-need-to-know

[9] Guarino Alessandro & Iasiello Emilio, « Imposing and evading cyber borders : the sovereignty dilemma », *Cyber, Intelligence, and Security*, June 2017, p. 4.

[10] Pauvert Bertrand, « L'entreprise, acteur de la sécurité nationale », *Sécurité globale*, 2007/1, p. 97-98, we translate.

[11] according to Belgian federal prosecutor Frédéric Van Leeuw: AFP, « La cybercriminalité, "un défi plus grand que le terrorisme" », *L'Echo*, 15 mai 2017, http://www.lecho.be/economie-politique/international-general/La-cybercriminalite-un-defi-plus-grand-que-le-terrorisme/9894181



« Verizon 2017 Data Breach Investigations Report », *op. cit.*, p. 3.

NO INTERNATIONALLY ACCEPTED LEGISLATION

As the legal frame for cybercrime is not ratified by a substantial number of states in a legislative instrument[12], and until most offensive actors like China[13] or Russia[14] are staying sideways, political or state judicial responses are insufficient[15] or inadequate[16]. An exception can be drawn up from the Council of Europe Convention on Cyber Crime, which shows how the leadership of the old continent can be inspiring. As a matter of fact, deterrence capability could only emerge if severe legal penalty is clearly defined as a well-known and commonly applied sanction for cyber misbehaviour, which should be controlled by an independent cyber agency[17].

For sure, cybercriminality is criminality first: from the biggest bandit to the smallest, financial seizure is considered by them as the main punishment while incarceration is regarded as accessory sentence[18]. However, due to the intrinsic nature of cyberspace, decentralized and omnipresent, law power may be diluted or restrained by national interests[19].

As borders regain interest in political and security domain[20], the difficulty to attribute the crime by identifying the actors is another barrier to an effective response, especially with terror groups. Thereby, a small level of certainty permit behind the scene diplomacy, a medium level of certainty allows public accusation,

[12] Guarino Alessandro & Iasiello Emilio, « Imposing and evading cyber borders : the sovereignty dilemma », *op. cit.*, p. 16; Cohen Matthew, Freilich Chuck & Siboni Gabi, « Four Big "Ds" and a Little "r": A New Model for Cyber Defense », *Cyber, Intelligence, and Security*, June 2017, p. 27.

[13] « EADS attaqué par des hackers chinois », *Le Monde*, 24th December 2013, http://www.lemonde.fr/technologies/article/2013/02/24/eads-attaque-par-des-hackers-chinois_1837971_651865.html; Charles Cuvelliez & Jean-Michel Dricot, « Le cyberéveil de l'Europe : à temps ou trop tard ? », *L'Echo*, 26th February 2013, http://www.lecho.be/opinions/analyse/le-cybereveil-de-l-Europe-a-temps-ou-trop-tard/9309341; *contra:* Douzet Frédérick, « Chine, États-Unis: la course aux cyberarmes a commencé », *Sécurité globale, ESKA*, 2013/1, p. 46-48.

[14] Nakashima Ellen, « U.S. said to be target of massive cyber-espionage campaign », *The Washington Post*, 10th February 2013, https://www.washingtonpost.com/world/national-security/us-said-to-be-target-of-massive-cyber-espionage-campaign/2013/02/10/7b4687d8-6fc1-11e2-aa58-243de81040ba_story.html; Establier Alain, « La sécurité numérique par ceux qui la conçoivent et la pratiquent », *op. cit.*, p. 31-45.

[15] Horwitz Sari, « Justice Department trains prosecutors to combat cyber-espionage », *The Washington Post,* 25th July 2012, https://www.washingtonpost.com/world/national-security/justice-department-trains-prosecutors-to-combat-cyber-espionage/2012/07/25/gJQAoP1h9W_story.html?utm_term=.651ac987654e

[16] Eudes Yves, « Hackers d'Etat », *Le Monde*, 19th February 2013, http://www.lemonde.fr/technologies/article/2013/02/19/hackers-d-etat_1834943_651865.html

[17] Cohen Matthew, Freilich Chuck & Siboni Gabi, « Four Big "Ds" and a Little "r": A New Model for Cyber Defense », *op. cit.*, p. 24-33; Raufer Xavier, « De la cyber-jungle au cybermonde », *op. cit.*, p. 5.

[18] Establier Alain, « La sécurité numérique par ceux qui la conçoivent et la pratiquent », *op. cit.*, p. 16-19.

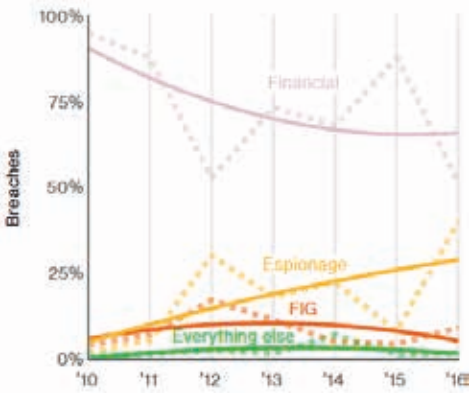
[19] Cohen Matthew, Freilich Chuck & Siboni Gabi, *ibid.*, p. 34; Establier Alain, « La sécurité numérique par ceux qui la conçoivent et la pratiquent », *op. cit.*, p. 31.

[20] Duez Denis, « La sécurisation des frontières extérieurs de l'union européenne: enjeux et dispositifs », *Sécurité globale*, 2012/1, p. 64.

whereas high level of certainty authorise legal and kinetic actions[21]. All range of policy responses have to be considered, from peaceful warning to armed strike, as neither (upper) proportionate response nor limited to cyberspace is mandatory[22].

Taking into account that data are legally considered as merchandise[23], the collection of data by control authorities and repressive services at borders to identify passengers who present a criminal or terrorist risk is a matter of importance. Not only how they treat it (e.g. via data mining) but also how they secure it. Knowing that Passenger Name Record (PNR) includes « every details of special requirement (…) detailed onboard meal requests, seat preferences, or medical assistance; potentially pointing out where a traveler went, when, why, with who, and with which financial support[24] », any breach in that database could be crucial. As state of emergency facilitates detention for terrorist suspicion[25] and because big data allows detecting and preventing threats before they concretise, with unclear legal frame, drifts in identity general databases are damageable mainly on presumption of innocence and freedom of movement as they lack to proportionality principle[26].

If Europe wants to stay at the cutting edge of data protection and privacy, it needs to implement similar rules for comparable services: by 2020, 90% of all text messages will transit through online platforms and no more via mobile networks[27]. In July 2016, the US National Institute of Standards and Technology's declared SMS as Two Factor Authentification (2FA) as insecure, because as well as voice calls they may be intercepted or redirected; and it's easy to subvert by tricking phone companies with some identity informations. Six months after the statement was published, companies such as NASA, Facebook, Toyota, are still using SMS as 2FA[28]…



« Verizon 2017 Data Breach Investigations Report », *op. cit.*, p. 5.

THE RISE OF CYBER-ESPIONAGE

According to Shawn Henry, former FBI's cyber sleuth, electronic spying peaks at unseen levels[29]. This cyber-espionage is the fact of states in 90% of cases[30], proceeding mostly by phishing (social), the use of malwares or backdoors and hacking. One way is through hostfiles[31] that we can consider as our computer adressbook, which if altered, calls the website hackers wants you to open instead of your usual one. This way your outcoming traffic can be redirected to servers they choose.

[21] Cohen Matthew, Freilich Chuck & Siboni Gabi, « Four Big "Ds" and a Little "r": A New Model for Cyber Defense », *op. cit.*, p. 24; *contra:* Limnéll Jarno, « Proportional Response to Cyberattacks », *op. cit.,* p. 47.
[22] Limnéll Jarno, *ibid.,* p. 47.
[23] Viola Roberto & Bringer Olivier, « Vers un marché unique numérique: faire de la révolution numérique une opportunité pour l'Europe », *Revue d'économie financière*, 2017/1, p. 240.
[24] Duez Denis, « La sécurisation des frontiers extérieurs de l'union européenne: enjeux et dispositifs », *Sécurité globale*, 2012/1, p. 69-70, we translate.
[25] Fontenoy Stéphanie, « Un étudiant de l'Ihecs arrêté en Turquie pour "terrorisme" », *L'Echo*, 4th August 2017, p. 3; Greenwald Glenn, *Nulle part où se cacher*, Jean-Claude Lattès, 2014, p. 399-344.
[26] Sente Arthur, « Tomorrowland, habitué du screening », *L'Echo*, 5th August 2017, p. 3.
[27] Viola Roberto & Bringer Olivier, *op. cit.*, p. 243-251.
[28] Pauli Darren, « Standards body warned SMS 2FA is insecure and nobody listened », *The Register*, 6th December 2016, https://www.theregister.co.uk/2016/12/06/2fa_missed_warning
[29] Horwitz Sari, « Justice Department trains prosecutors to combat cyber-espionage », *op. cit.*
[30] « Verizon 2017 Data Breach Investigations Report », *Verizon*, 27th April 2017, 10th Ed, http://www.verizonenterprise.com/resources/reports/rp_DBIR_2017_Report_en_xg.pdf, p. 43.
[31] Arntz Pieter, « Host file hijacks », *Malwarebytes*, 19th December 2016, https://blog.malwarebytes.com/cybercrime/2016/09/hosts-file-hijacks

Worryingly, Edward Snowden's release of NSA intern documents proved the agency spied not only international crime under terrorism prevention pretext, but that the final aim is also military, political, diplomatic or socio-economical[32]! We observe in economical intelligence that there is no enemy or friend and that we have to keep adverse spies busy during detente periods, because «we need our allies but they are sometimes closely interested to what we do» and it is forbidden to say they can steal us[33].

SELF-DRIVEN AIRCRAFT HACKING

Even non connected target can be neutralised, such as USS Donald Cook ship that were fled over by a Sukhoï-24 in 2014[34], and many others publicly unrevealed. As self-driven aircraft and Unmanned Combat Aerial Vehicle (UCAV) are progressively taking part of aerospace and adding more discreet material points of entry, the peaceful hack of an airplane from the passenger seat through the intern entertainment system manipulation[35] raises many questions. First of all, why is there no real condition test of an electromagnetic-attack on the *entire* components of F-16 successors? Considering the error threshold admitted for the test that were actually done on *some* components, do we take in account *concomitant* risks in vulnerability scenarii? Given that aircrafts are thunder safe and nuclear tested, does a *sufficient* charge nevertheless neutralise them? If it does, it is worrying that constructors are aware of electronic targeting and preparing new models dedicated[36], but currently selling precious fighters that aren't sufficiently equipped to counter a strong or targeted electromagnetic and/or electronic threat!

In this collateral menace, every indirect way to neutralise a network has to be considered[37]. On one hand, IoT represents billions of devices without antivirus, sometimes without updatable software in case of leak, with too simple hardware architecture, and above all always connected! To make a long story short, IoT personify perfect targets that can be used as potential relays for hackers[38].

On the other hand, infiltration can be done by drones to deceive a plane system via its external sensors, copying technical characteristics of industrials Application programming Interface (API) to trick central unity, using cryptography; or by the external ground communication, breaking or scrambling radio reception, inducing pilot to do something by copying his squadron's chief voice[39]; the automatic upgrade, or the electric grid… We have to think dual, include real-time situational picture[40], have a global vision on the fragility of our vital infrastructures (telecommunications, energy, transport), whether they are civil or military. Because deep attack can target and cause the fall of water distribution system, a plant, railroad[41] or flights regulation center. Their breakability resides in old routers, passwords like «admin admin», lack of human awareness of personnel, etc.

Collateral knowledge is the key in an expertise environnement where many people hold multidisciplinary information[42], particularly when veil of ignorance is regularly raised between military intelligence and political echelon: policymakers lack of transparence about their policy while they should ask questions about more than just data, whereas intelligence officers must formulate advices[43]. It is obvious that artificial intelligence (AI) can scan the risks and even intervene amid decisional process, reducing its cost and time[44], but it was once coded by a human,

32 Delesse Claude, «La NSA, «mauvais génie» du cybermonde ?», *op. cit.*, p. 69.
33 Establier Alain, «La sécurité numérique par ceux qui la conçoivent et la pratiquent», *op. cit.*, p. 27-51, we translate.
34 Muller Feuga Philippe, «Cyberespace, nouvelles menaces et nouvelles vulnérabilités», *op. cit.*, p. 93-94.
35 Al Bouchouari Younes, «Hacker un avion depuis son siège passager, tranquille», *L'Echo*, 19th May 2015, http://www.lecho.be/entreprises/aviation/hacker-un-avion-depuis-son-siege-passager-tranquille/9634997
36 Mader Georg, «"Growler" edition is next plan for Gripen, says senior SAAB exec», *Defence IQ*, September 2015, http://internationalfighter.iqpc.co.uk/media/1001045/50607.pdf
37 Muller Feuga Philippe, «Cyberespace, nouvelles menaces et nouvelles vulnérabilités», *op. cit.*, p. 93.
38 Raufer Xavier, «De la cyber-jungle au cybermonde», *op. cit.*, p. 7.
39 Raufer Xavier, *ibid.*, p. 9.
40 Duez Denis, «La sécurisation des frontières extérieurs de l'union européenne: enjeux et dispositifs», *op. cit.*, p. 72.
41 Establier Alain, «La sécurité numérique par ceux qui la conçoivent et la pratiquent», *op. cit.*, p. 44-47.
42 Riles Annelise, «Legal reasoning in the global financial markets», *University of Chicago Press*, 2011.
43 Siman-Tov David & Hershkovitz Shay, «A Cooperative Approach between Intelligence and Policymakers at the National Level: Does it Have a Chance?», *Cyber, Intelligence, and Security,* Vol. 1, N° 2, June 2017, p. 98-101.
44 Gheur Charles, «L'intelligence artificielle va bouleverser la Justice», *L'Echo*, 30th May 2017, p. 11.

Mader Georg, « "Growler" edition is next plan for Gripen, says senior SAAB exec », *op. cit.*

keeping its misjudgement, at the contrary of a pool of experts knowledge, whose qualitative risk assessments workshshops related on white papers can't be hacked as easily… Indeed, when those meetings happen, they came to the conclusion that we really need to redesign deeply the future of our system architecture with the help of industrials! « Should we stay on completely flat systems whereby guidance part of the ship is accessible from any PC, thus reachable by an attacker[45]? » asks french armies Vice-Admiral and Cyber defence general officer at military staff. Every weapon, vessel or aircraft shall be conceived properly, with specific structure.

European countries are considering the investment in a non piloted fighter[46], a sensitive project from a security perspective: the damages of a theft would be worrisome, not because of the cost of the aircraft, but due to material access to technology. These UCAV will give more images to treat than israelian drones currently do: up to 7 of them are flying for a total of 50.000 hours per year in the Skyeye program, each of them covering a 10 km^2 area, transmitting terabytes of air-ground encrypted data. Up to 10 operators can access the system simultaneously, looking backward, forward, or focus, with the strategic possibility to target in time and space a car in the city, from where it came to where it is going. During events or in case of specific threats, the area covered can be even larger if precision is not a matter of importance, as the UAV can fly higher. But the flow of images to analyse and the stockage capacities are present issues, forcing the UAV to regularly upload the content on air, which represents a vulnerability at the heart of every communication. We should never forget simple things such as the more an entity communicate, the less it is *safe*, just to think one moment about always connected devices, or new generation of fighters… Than, from a *security* point of view, the length of time an adversary can grab access to data matter, hence the quality of encryption is decisive. The distinction goes beyond the scope of CIA definition: if security flaws are tolerable, military speaking safety risks are not: while the first only impact *confidentiality* (C), the last puts lives and infrastructures in danger by affecting *integrity* (I) or *availability* (A).

Actually, AI could be a way to resolve the insufficient qualified workers in imagery treatment, or linguists, to manage the rising number of satellite photos, radar intercepts and military communications. Automated treatment in big data allows confidentiality and

[45] Establier Alain, « La sécurité numérique par ceux qui la conçoivent et la pratiquent », *op. cit.*, p. 45, we translate.
[46] Gosset Olivier, « Le délicat chantier du chasseur européen », *L'Echo*, 15 juillet 2017, p. 8.

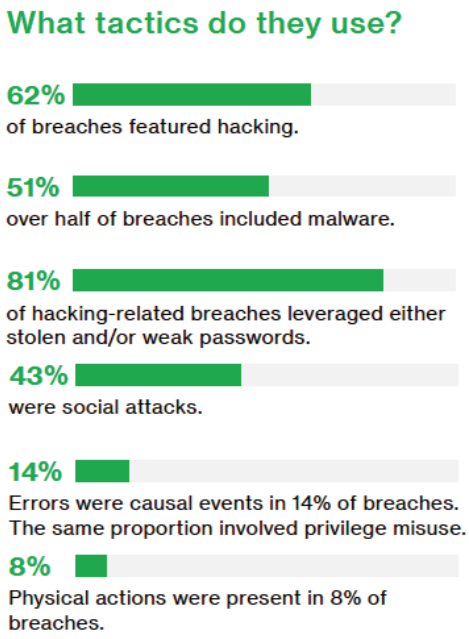
pertinent search to submit the right information to analysts[47].

FASTER CONNECTION, HIGHER SECURITY NEEDS

« All of what we need, is an access to an high-speed internet connection[48]. » It could have been pronounced by a hacker, but those words are from Jean-Claude Juncker[49]. At the contrary, belonging to cyber experts: « hyper connectivity + hyper competitivity = hyper vulnerability[50]. » Indeed, the improvements to data processing and speed connection are the best way to improve productivity, but this course leads to rising security concerns. Digital deceleration isn't the right answer as the technological gap causes comparative disadvantages to economies[51].

REMEDIES: PREVENTION AND REPORTING

Lack of protection and quick reaction to breaches are the black spot listed by IT experts: corporations often deny incident or minimise risk[52] in place of facing it with experts. The development of a response plan in case of cyber incident is recommended by intelligence agencies; intimating to apply forensic analysis and law enforcement, implicate legal advisors, and have a non IT reply. Although information sharing on data breach[53] is one of the key for Internet Service Provider (ISP) and antivirus developer to avoid (re)iteration of leaks[54], the bad reputation mark has often prevented companies to report; for the good safe of cybercriminals[55]. When it is not business confidentiality that restrain them[56]…



« Verizon 2017 Data Breach Investigations Report », *op. cit.*, p. 3.

One vulnerability noticeable is the absence of short managerial circuit in the core of States. Another is between them and entreprises, in a bottom up approach: upholding quick, adaptative and reactive answer to threats. A third one is human factor which can be easily misled (usually by phishing) and underline the social engineering necessity. Last but not least is the lack of global consideration of components, which no system administrator can entirely handle: between

[47] Establier Alain, *ibid.*, p. 29.
[48] Viola Roberto & Bringer Olivier, « Vers un marché unique numérique: faire de la revolution numérique une opportunité pour l'Europe », *op. cit.*, we translate.
[49] « Speech on the state of the Union: towards a better Europe – which protects, give means to react and defend », 14th September 2016.
[50] Establier Alain, « La sécurité numérique par ceux qui la conçoivent et la pratiquent », *op. cit.*, p. 37.
[51] Muller Feuga Philippe, « Cyberespace, nouvelles menaces et nouvelles vulnérabilités », *op. cit.*, p. 87-89.
[52] Establier Alain, « La sécurité numérique par ceux qui la conçoivent et la pratiquent », *op. cit.*, p. 18.
[53] « Verizon 2017 Data Breach Investigations Report », *Verizon*, 27th April 2017, 10th Ed, http://www.verizonenterprise.com/resources/reports/rp_DBIR_2017_Report_en_xg.pdf, p. 63; Cohen Matthew, Freilich Chuck & Siboni Gabi, « Four Big "Ds" and a Little "r": A New Model for Cyber Defense », *op. cit.*, p. 33.
[54] Cuvelliez Charles, « Vous vous croyez à l'abri des pirates ? », 14th October 2011, *L'Echo*, http://www.lecho.be/opinions/analyse/Vous-vous-croyez-a-l-abri-des-pirates/9115563
[55] Horwitz Sari, « Justice Department trains prosecutors to combat cyber-espionage », *op. cit.;* Establier Alain, « La sécurité numérique par ceux qui la conçoivent et la pratiquent », *op. cit.,* p. 23.
[56] Limnéll Jarno, « Proportional Response to Cyberattacks », *op. cit.,* p. 46.

« Verizon 2017 Data Breach Investigations Report », *op. cit.*, p. 3.

human conceptional errors from the historic creation of networks in 1969; to software coding flaws or back doors; and hardware vulnerabilities to electromagnetic shocks[57]. Undeniably, cost of security measures is often a curb to their implementation for small actors.

INTERNATIONAL COOPERATION

International cooperation is confronted to sovereignty obstacles or justified mistrust[58]. However, the (contested[59]) transnational nature of cyberspace asks for a coordinated response[60]. Applying subsidiarity principle, Europe's budget could assume a unique cyber agency to be able to counter correctly the future cyberthreats that linges over every separate member state: there's no better level to intervene than the regional in this domain[61]. We could do the analogy with a network firewall: to protect the computers inside, it has to be placed at the frontier. The border of our network is European, subnetwork of the occidental cyber realm.

Parcelling is at work not only in entreprises network to protect them from a wide scale infection[62]. We could apply this principle broadly to cities, countries and regions. And have real time situational images to stop haemorrhage, put the infected targets offline, and restore backup of our infrastructures with secondary networks.

DO NOT RELY ON TECHNOLOGY

Hardware and software should not be provided from the same company to improve architecture resilience[63], avoids back-doors and accelerate problem isolation. Skilled and regularly trained to cybersecurity managers are lacking[64]. Having offline alternative and physical mean to block attack: think about strategies that do not involve technology (e.g. four eyes principle: proceedings approved by colleagues, biometric badges, access denied if any doubt, cameras[65]).

Human awareness when using IoT or simply mobile devices is more crucial then ever: in a rural condition test, with little radio interference (which correspond to much of battlefield situations), a WiFi signal was received by a Venezuelan expert at a distance of 382 km[66] ! Forgetting to put all your waves off before

[57] Muller Feuga Philippe, « Cyberespace, nouvelles menaces et nouvelles vulnérabilités », *op. cit.*, p. 88-92.
[58] F.D., « Trump Jr. avoue avoir rencontré une avocate russe », *L'Echo*, 11 juillet 2017, p. 9.
[59] Guarino Alessandro & Iasiello Emilio, « Imposing and evading cyber borders : the sovereignty dilemma », *op. cit.*, p. 6-7.
[60] Cohen Matthew, Freilich Chuck & Siboni Gabi, « Four Big "Ds" and a Little "r": A New Model for Cyber Defense », *op. cit.*, p. 27.
[61] Guarino Alessandro & Iasiello Emilio, « Imposing and evading cyber borders : the sovereignty dilemma », *op. cit.*, p. 15; Cohen Matthew, Freilich Chuck & Siboni Gabi, *ibid.*, p. 33; Establier Alain, « La sécurité numérique par ceux qui la conçoivent et la pratiquent », *op. cit.*, p. 31.
[62] Witvrouw François, « Comment éviter de vous faire hacker?", *L'Echo,* 30 juin 2017, http://www.lecho.be/economie-politique/international-general/Comment-eviter-de-vous-faire-hacker/9909604?highlight=cybersecurite
[63] Cohen Matthew, Freilich Chuck & Siboni Gabi, « Four Big "Ds" and a Little "r": A New Model for Cyber Defense », *op. cit.*, p. 35.
[64] Johnson Thomas A., « Critical Infrastructures, Key Assets: A Target-Rich Environment », *Cybersecurity - Protecting Critical Infrastructures from Cyber Attack and Cyber Warfare*, CRC Press, 2015, p. 59; Radichel Teri, « Case Study: Critical Controls that Could Have Prevented Target Breach », *SANS Institute*, 2014, http://www.sans.org/reading-room/whitepapers/casestudies/case-study-critical-controls-prevented-target-breach-35412, p. 25; Establier Alain, « La sécurité numérique par ceux qui la conçoivent et la pratiquent », *op. cit.*, p. 34.
[65] Scharff Christine, « Le sabotage de Doel 4 reste un mystère », *L'Echo*, 4th August 2017, p. 15.
[66] Electronic Frontier Fondation, « The Problem with Mobile Phones », *Surveillance Self-Defense*, 10th February 2015, https://ssd.eff.org/en/module/problem-mobile-phones

quitting a position can reveal all the movements of the troops, their regular patrols, only because one soldier forgot its bluetooth on its personal Fitbit which was scanned nearby…

Counter-manipulation techniques coming from communication theory can ben envisaged to counterspell the effets of data manipulation.

CYBER-RESILIENCE

Resilience is the ability to come back to a normal situation after a threat[67]. In the cyber realm, it means visiting the enclosure, accept its tolerable failures, improve the critical ones, and be prepared for an invasion in case of emergency so that at any moment, the generator is ready to take over.

Even if there will always be unexpected failure, improve technological ressources with concentrate efforts on critical infrastructures. The key resides on resilient systems that can quickly be rebooted or back-up, reseted in a temporary basic configuration with vital but urgent needs. Different part of system with different lengths of rebooting depending of their needs should be progressing through this recovery process and regularly tested in real threat environment.

Preventing major attack is the ultimate aim as minor do not have any damageable impact: prioritise threat defence is part of cost and risk management. It's hard to reach such a level of complexity (and damages correlated) needed in offensive response to an attack so that retaliation is efficient, a reason why defence is a good investment in any case for small and middle actors[68]. Furthermore, the response to cyberattacks is still broadly considered as an untested phenomenon[69].

SIMPLE BUT CRUCIAL TECHNOLOGICAL UPDATE

Due to budgetary constraint[70], technological advance is the laggard of our infrastructures. Israel stays a leader not only in cyber « by building a military that relies on quality rather than quantity. It invests heavily in high-tech weaponry, recruits its armed forces through mandatory national service, and maintains a reserve force comprised of a significant portion of the country's population[71]. »

[67] Establier Alain, « La sécurité numérique par ceux qui la conçoivent et la pratiquent », *op. cit.*, p. 36.
[68] Cohen Matthew, Freilich Chuck & Siboni Gabi, « Four Big "Ds" and a Little "r": A New Model for Cyber Defense », *op. cit.*, p. 29-30.
[69] Limnéll Jarno, « Proportional Response to Cyberattacks », *op. cit.,* p. 37.
[70] Establier Alain, « La sécurité numérique par ceux qui la conçoivent et la pratiquent », *op. cit.*, p. 26.
[71] Kaura Vinay, « Comparative Assessment of Indian and Israeli Military Strategy in Countering Terrorism », *Cyber, Intelligence, and Security*, Vol. 1, N° 2, June 2017, p. 112.

CONCLUSION

In an permanently connected world, not only should we be prepared to thwart a on the ground electronic Pearl-harbour scenario. We should consider the possibility that it will happen that all our fleet will be on air and available, but not controllable. Or worse: being attacked by our own vessels… We shall have reaction plans and trained not only IT chiefs to the situation whereas no computer is responding, even the most critic one, trustworthy, or newly protected. We should learn how to react quickly without relying on technology and have alternatives putted in place long time ago, like analogic cutting-circuit or human to human communication.

Even the situational screens can be confusing at a point where data are corrupted from their database, targets potentially modified and therefore the issue of every mission compromised. This is a reason why conventional confirmation, on the ground and eye seeing people are crucial. But secured way of communication that do not transit through the internet or any transatlantic cable nor satellite communication that can be intercepted and manipulated is also a challenge. The architecture has to be though in a way that security is at the core of the construction, to the contrary of the actual margin added structure.

End to end encryption is no longer safe as intelligence agencies have the means to broke them. Communications cannot be safe for all if anyone has placed a backdoor and that the key can be easily stolen. Just consider one moment all those tools, not a few, but all this armada being in the wrong hands after an exploit or an insider theft in one of these agency. China or Russia is a little threat in comparison to the capacity of any little smart guy able to breach in NSA gadgets.

Would we be so tolerant about letting the nuclear weapons in the hands of any nation? Actually, cyberweapons have the power tobe nuclear, bacteriologic, financial, communicational, and logistic at the same time, due to the interconnectivity at the core of our networks. We did not think about security when building them: we though about connectivity. Our politics still do… It is time to change our minds.

BIBLIOGRAPHY

- « Counter-terrorism: framing jihadist networks with analytics », *SAS*, 26th - 28th June 2017
- « Deep learning », Dell EMC, 2017
- « GPU accelerated computing technology for security analytics », Dell EMC, 2017
- « COMINT & C-ESM information fusion », Saab Medav Technologies GmbH
- *Le guide complet du piratage*, Edigo, 2009
- « Verizon 2017 Data Breach Investigations Report », *Verizon*, 27th April 2017, 10th Ed, http://www.verizonenterprise.com/resources/reports/rp_DBIR_2017_Report_en_xg.pdf
- « EADS attaqué par des hackers chinois », *Le Monde*, 24th December 2013, http://www.lemonde.fr/technologies/article/2013/02/24/eads-attaque-par-des-hackers-chinois_1837971_651865.html
- AFP, « La cybercriminalité, "un défi plus grand que le terrorisme" », *L'Echo*, 15 mai 2017, http://www.lecho.be/economie-politique/international-general/La-cybercriminalite-un-defi-plus-grand-que-le-terrorisme/9894181
- « Building an Effective European Cyber Shield », European Political Strategy Centre, 8th May 2017, https://ec.europa.eu/epsc/publications/strategic-notes/building-effective-european-cyber-shield_en
- Arpargian Nicolas, *La cybersécurité*, PUF, Coll. Que sais-je?, 2010
- Arntz Pieter, « Host file hijacks », *Malwarebytes*, 19th December 2016, https://blog.malwarebytes.com/cybercrime/2016/09/hosts-file-hijacks
- Bensoussan-Brulé Virginie & Torres Chloé, *Failles de sécurité et violation de données personnelles*, Larcier, 2016
- Al Bouchouari Younes, « Hacker un avion depuis son siège passager, tranquille », *L'Echo*, 19th May 2015, http://www.lecho.be/entreprises/aviation/hacker-un-avion-depuis-son-siege-passager-tranquille/9634997
- Boyer Bertrand, *Dictionnaire de la Cybersécurité et des Réseaux*, Nuvis, 2015
- Cohen Matthew, Freilich Chuck & Siboni Gabi, « Four Big "Ds" and a Little "r": A New Model for Cyber Defense », *Cyber, Intelligence, and Security*, Vol. 1, n°2, June 2017, p. 21
- Cox Ingemar J., Miller Mattew L., Bloom Jeffrey A., Fridrich Jessica & Kalker Ton, *Digital Watermarking and Steganography*, 2d ed., Morgan Kaufmann, 2011
- Cuvelliez Charles, « Vous vous croyez à l'abri des pirates ? », 14th October 2011, *L'Echo*, http://www.lecho.be/opinions/analyse/Vous-vous-croyez-a-l-abri-des-pirates/9115563
- Cuvelliez Charles & Dricot Jean-Michel, « Le cyberéveil de l'Europe : à temps ou trop tard ? », *L'Echo*, 26th February 2013, http://www.lecho.be/opinions/analyse/le-cybereveil-de-l-Europe-a-temps-ou-trop-tard/9309341
- Delesse Claude, « La NSA, «mauvais génie» du cybermonde ? », *Sécurité globale*, ESKA, 2016/4, n°8, p. 67-104
- Delesse Claude, « Note de lecture - NSA, l'histoire de la plus secrète des agences de renseignement », *Sécurité globale*, ESKA, 2016/4, n°8, p. 105-106
- Douzet Frédérick, « Chine, États-Unis: la course aux cyberarmes a commencé », *Sécurité globale, ESKA*, 2013/1, n°23, p. 43-51
- Duez Denis, « La sécurisation des frontières extérieurs de l'union européenne: enjeux et dispositifs », *Sécurité globale*, ESKA, 2012/1, n°19, p. 63-76
- Electronic Frontier Fondation, « The Problem with Mobile Phones », *Surveillance Self-Defense*, 10th February 2015, https://ssd.eff.org/en/module/problem-mobile-phones
- Establier Alain, « La sécurité numérique par ceux qui la conçoivent et la pratiquent », *Sécurité globale, ESKA*, 2016/4, n°8, p. 11-56
- Eudes Yves, « Hackers d'État », *Le Monde*, 19th February 2013, http://www.lemonde.fr/technologies/article/2013/02/19/hackers-d-etat_1834943_651865.html
- Fontenoy Stéphanie, « Un étudiant de l'Ihecs arrêté en Turquie pour "terrorisme" », *L'Echo*, 4th August 2017, p. 3
- F.D., « Trump Jr. avoue avoir rencontré une avocate russe », *L'Echo,* 11th July 2017
- Ghernaouti Solange, *Cybersécurité - sécurité informatique et réseaux*, Dunod, 5th ed., 2016
- Gheur Charles, « L'intelligence artificielle va bouleverser la Justice », *L'Echo*, 30th May 2017, p. 11
- Greenwald Glenn, *Nulle part où se cacher*, Jean-Claude Lattès, 2014.
- Gosset Olivier, « Le délicat chantier du chasseur européen », *L'Echo*, 15 juillet 2017, p. 8
- Guarino Alessandro & Iasiello Emilio, « Imposing and evading cyber borders: the

sovereignty dilemma», *Cyber, Intelligence, and Security*, Vol. 1, N° 2, June 2017, p. 3
- H. An., «La criminalité constatée a baissé de 5% en un an», *La Libre Belgique*, 28th June 2017
- Herminaire Jean-Christophe, «De moins en moins de criminalité en Belgique», *L'Avenir*, 28th July 2017, p. 2
- Horwitz Sari, «Justice Department trains prosecutors to combat cyber-espionage», *The Washington Post,* 25th July 2012, https://www.washingtonpost.com/world/national-security/justice-department-trains-prosecutors-to-combat-cyber-espionage/2012/07/25/gJQAoP1h9W_story.html?utm_term=.651ac987654e
- Johnson Thomas A., «Critical Infrastructures, Key Assets: A Target-Rich Environment», *Cybersecurity - Protecting Critical Infrastructures from Cyber Attack and Cyber Warfare*, CRC Press, 2015, p. 33
- Kaura Vinay, «Comparative Assessment of Indian and Israeli Military Strategy in Countering Terrorism», *Cyber, Intelligence, and Security*, Vol. 1, N° 2, June 2017, p. 107
- Lagast Cedric, «Inbrekers slaan nu toe vanachter de computer», *Het Nieuwsblad*, 28th July 2017, p. 7
- Lagast Cedric, «Criminelen slaan toe vanachter computer - Politie heeft handen vol met cybercrime», *Gazet van Antwerpen*, 28th July 2017, p. 6
- Leonetti Xavier, *Guide de cybersécurité - Droits, méthodes et bonnes pratiques*, L'Harmattan, 2015
- Limnéll Jarno, «Le cyber change-t-il l'art de la guerre ?», *ESKA*, 2013/1, n°23, p. 33-41
- Limnéll Jarno, «Proportional Response to Cyberattacks», *Cyber, Intelligence, and Security*, June 2017, Vol. 1, n°2, p. 37-52
- Lucat Jean, «La sécurité informatique pour l'usager de base. Un expert de terrain, dix fondamentaux», *Sécurité globale*, ESKA, 2016/4, n°8, p. 57-65
- Mader Georg, «"Growler" edition is next plan for Gripen, says senior SAAB exec», Defence IQ, September 2015, http://internationalfighter.iqpc.co.uk/media/1001045/50607.pdf
- Muller Feuga Philippe, «Cyberespace, nouvelles menaces et nouvelles vulnérabilités», *Securité globale*, ESKA, 2017/1, n° 9, p. 83-95
- Nakashima Ellen, «U.S. said to be target of massive cyber-espionage campaign», *The Washington Post*, 10th February 2013, https://www.washingtonpost.com/world/national-security/us-said-to-be-target-of-massive-cyber-espionage-campaign/2013/02/10/7b4687d8-6fc1-11e2-aa58-243de81040ba_story.html
- Pauvert Bertrand, «L'entreprise, acteur de la sécurité nationale», *Sécurité globale*, ESKA, 2007/1, n°9, p. 97-104
- Pauli Darren, «Standards body warned SMS 2FA is insecure and nobody listened», *The Register*, 6th December 2016, https://www.theregister.co.uk/2016/12/06/2fa_missed_warning
- Pillou Jean-François & Lemainque Fabrice, *Tout sur les Réseaux et Internet*, Dunod, 3rd ed. 2012
- Radichel Teri, «Case Study: Critical Controls that Could Have Prevented Target Breach», *SANS Institute*, 2014, http://www.sans.org/reading-room/whitepapers/casestudies/case-study-critical-controls-prevented-target-breach-35412
- Raufer Xavier, «De la cyber-jungle au cybermonde», *Sécurité globale, ESKA*, 2016/4, n°8, p. 5-10
- Raufer Xavier, «Démons et merveilles du "prédictif": une bonne fois pour toutes…», *Sécurité globale, ESKA*, 2016/4, n°8, p. 107-120
- Richet Jean-Loup, *Cybersecurity Policies and Strategies for Cyberwarfare Prevention*, IGI, 2015
- Riles Annelise, «Legal reasoning in the global financial markets», *University of Chicago Press*, 2011
- Scharff Christine, «Le sabotage de Doel 4 reste un mystère», *L'Echo*, 4th August 2017, p. 15
- Schönberger Viktor Mayer & Cukier Kenneth, *Big Data, La révolution des données en est marche*, Robert Laffont, 2014
- Sente Arthur, «Tomorrowland, habitué du screening», *L'Echo*, 5th August 2017, p. 3
- Siman-Tov David & Hershkovitz Shay, «A Cooperative Approach between Intelligence and Policymakers at the National Level: Does it Have a Chance?», *Cyber, Intelligence, and Security,* Vol. 1, N° 2, June 2017, p. 85
- Singer P.W. & Friedman Allan, *Cybersecurity and cyberwar - what everyone needs to know,* Oxford University Press, 2016
- Sherr Ian, «WannaCry ransomware: Everything you need to know», *Cnet,* 19th May 2017, https://www.cnet.com/news/wannacry-wannacrypt-uiwix-ransomware-everything-you-need-to-know
- Shinotsuka Hiroshi, «How attackers steal private keys from digital certificates», *Symantec*, 22th February 2013, https://www.symantec.com/connect/blogs/how-attackers-steal-private-keys-digital-certificates
- Sternberg David, «Framing the Cyberthreat through the Terror-Ballistics Analogy», *Cyber, Intelligence, and Security*, Vol. 1, N° 2, June 2017, p. 125

- Stevenson Mitchell, Terrell Karen, Cramer Mark & Khatri Vijay, « How Advanced Analytics can increase Mission & Security Effectiveness », *SAS*, 26th - 28th June 2017
- Stuart Andrew, « WannaCry: Smaller businesses are at great risk », *HelpNetSecurity*, 18th May 2017, https://www.helpnetsecurity.com/2017/05/18/wannacry-smb-risk
- Viola Roberto & Bringer Olivier, « Vers un marché unique numérique : faire de la révolution numérique une opportunité pour l'Europe », *Revue d'économie financière*, 2017/1, n°125, p. 239-254
- Witvrouw François, « Comment éviter de vous faire hacker ? », *L'Echo,* 30 juin 2017, http://www.lecho.be/economie-politique/international-general/Comment-eviter-de-vous-faire-hacker/9909604?highlight=cybersecurite
- Witvrouw François, « Nouvelle cyberattaque d'ampleur mondiale », *L'Echo*, 28th June 2017, p. 16

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