INFO FLASH
Finabel
European Army Interoperability Centre

Forming New Generation of Cyber-Fighter: How Armies Are Trying to Improve Military's Education and Training Panoply on Cybersecurity Issues.

WRITTEN BY BRIANE MEZOUAR

hhttps://www.flickr.com/photos/army-cyber/44751802145/in/dateposted/

INFO FLASH
Finabel
European Army Interoperability Centre
Forming New Generation of Cyber-Fighter: How Armies Are Trying to Improve Military's Education and Training Panoply on Cybersecurity Issues
By Briane Mezouar

The War in Ukraine as an eyes-opener

As cyber security became a more prominent issue in modern conflict, armies must adapt education and training given within schoolhouses to their military. Some of them already reviewed their program and infrastructure to rise substantially the level of skills and acknowledge detained by their soldier. Although the recent aggression of Russia gives some food for thought and helps West's armies to incorporate lessons from the battlefield, many states did not waited for a high-intensity conflict to develop their cyber security architecture and capacities.

As it was the first major conflict involving large-scale cyber operations (Lewis, 2022), the war in Ukraine also works as a strong reminder for the West that cyber and electrical warfare is appealing to play a more prominent role in the near future (Gill, 2022). Many services learn a lot from this conflict in which cyber tends to have a key role besides purely kinetic actions. Their interest in having a well-trained and educated personnel increased if we take into account the increasing complexity and scale of those cyber-operations. Auditioned in July by the National Defence and Armed Forces Commission, the French National Defence General Secretary/ Secrétaire Général de la Défense Nationale (NDGS/SGDN) claims that since the beginning of 2021, we assist to an exploding « number of attacks and file extractions, espionage, sabotage attacks by states and state proxies » (i.e §3, p.5, Bouillon, 2022). He summarises cyber attacks as those made from the weak to the powerful (« du faible au fort »), concluding that facing those attacks, we « do not have much of an answer » (§4, p.6, Bouillon, 2022).

Nevertheless, the Ukraine war case shows us that a well-forewarned, prepared and assisted state with cooperative relationships, will strengthen its defensive capacities. One claims that a « well-prepared and energetic defence can have the advantage over offence in cyberspace ». Such defensive abilities (asides from purely technological capacities) begin first with the training and education of the personnel. Thus, the war in Ukraine seems to act as an eyes-opener for lots of states on the importance of having an army capable of quickly responding to cyber threats, even in a high-intensity conflict, and therefore, have enough skilful personnel to compete on the higher level of engagement (Gill, 2022). Some recent events should remind us of the importance of having a well-trained personnel on cyber issues, especially in such a congested and contested environment.

Ten days ago, NATO’s and EU’s member state, Estonia, was targeted with what seems to be « the most expensive cyber-attack » since its first ever hybrid warfare act in 2007, according to the Government (Davies, 2022). Learning from the past, Estonia had since then built a strong cyber defence system and structures, allowing the country to rise to the fourth place on the Global Cybersecurity Index Global Score and Ranking (i.e Global Index Security, International Communication Union, 2020). Following the access blocking to more than 200 state and private Estonian institutions, the pro-Russian hacker group Killnet claims the paternity of this manoeuvre. Another major cyber attack against the West’s interests and infrastructures was the sabotage of VISAT satellite internet provider's service earlier this year. U.S National Security Agency and l’Agence Nationale de Sécurité des Systèmes Informatiques (ANSSI) claim it was the work of Russian-state-backed hackers in an attempt to sever Ukrainian communications on the battlefield (Pearson, Satter, Bing, Schectman 2022). We can also note that between 24 February and April, more than 15 major cyber attacks were listed. They include among others; an attack on the communication systems of the Kyiv Post and the KA-SAT satellite network; an IssacWiper attack against government websites; a cyber-attack targeting a border control station; an attacks on Ukraine's digital infrastructure (blocking access to financial services and energy); a malware launched against governmental and financial websites; and non-government, charity and aid organisations (i.e CaddyWiper that infiltrate the systems of several organisations in the financial sector); some phishing attacks against government services; attacks against telecommunication service providers; dissemination of false message ad deep-fake video; phishing emails targeting the government and the military; cyber-assaults targeting Ukrtelecom and WordPress sites; extraction of sensitive information and user credentials from the Ukrainian government and media entities (§2, p.2, European Parliament, 2022). From the word of General Paul Stanton, the Army Cyber Center of Excellence chief, this invasion gave the Center (and Allies services) , the opportunity to « incorporate lessons learned from the Russian invasion of Ukraine into its schoolhouse curriculum » (Gill, 2022).

The risk of a lack of training and acknowledging : a persistent issue

Taken isolated, cyber-attacks are eventually statistically less likely to support retaliation with force escalation into a kinetic response (Cone, B.D., Thompson, M.F., Irvine, C.E., Nguyen, T.D, 2006). But as we observe the expansion of the hybrid warfare environment the major powers are evolving over decades, the slow shift from twenty years of asymmetric conflicts against non-state actors to actual (and future) high-intensity conflicts, push states to improve the quality of their staff's education on cybersecurity issue and fill gaps, sometimes within different corps of their army and between « traditional » warfare fields and cyber warfare. Thus, the equation on the improvement of states' cybersecurity capacities cannot be solved as long as the critical point of the grey matter available isn't treated. One note the current and persistent lack of qualified individuals and awareness of cyber security issues, mostly in the EU (Yamin, M.M., Erdodi, L., Torseth, E., Katt, B., 2022). In his 2020 report, the Global Cybersecurity index pointed out that effective mechanisms and institutional structures at the national level are necessary for building cybersecurity resilience. But even if a significant number of countries are yet to develop sector-specific training, a lot of countries lack programmes tailored toward specific sectors or professions such as law enforcement, legal actors, SMEs, private companies, and government officials (i.e p.17; International Telecommunication Union, 2020). Note that the issue goes far beyond sole military personnel as the scope of cyberattack is wide enough to engage and target random citizens occupying strategic positions, public figures, leaders, and civil strategic structures. Thus, it's also about how those people are trained to face cyberattacks, and counter them with appropriate and effective resources and capacities. As a FINABEL study shows, (i.e p.10 FINABEL, 2018), Cyber Expert Level Courses and Extra-muros training in civilian universities or private companies are better implemented than any other type of cyber training among Member States. It clearly shows that providing basic cyber training to entry personnel seems to have become a pressing concern for member states. But the least developed course in cyber for all Finabel Member States is the "Advanced training course during a military career." Thus, the problem relies on both issues. Improve civil society (and its structure) education while pushing further military personnel education by provides them advanced training.

As major military power cannot afford anymore to occult the overall importance of that issue for armies corps, states seem to have chosen to rethink the way they educate and pass knowledge on cyber-security topics. Many states act on a dual approach based on capacities development (awareness campaigns, training, education) and cooperation (partnerships between agencies, firms, and countries). They also melting the civil and military sphere into interdisciplinary and multi-level training structures, so they can push their progress in personnel cyber education and training. Finally, they use purely military program (starting since the military schoolhouse) or renewed operational strategic approach on cyber operations, and cultural environment. Those strategies are extended by international cyber defence assistance based on cooperation.

Readiness and operationally of personnel: Leveling-up random soldier's cyber knowledge by training, education

Since the war in Ukraine provides lessons on the value of electronic warfare, U.S Army recently decided to launch a program to better train cyber forces and close technology skill gaps across the military. It aims at changing the current curriculum, approach and assessment strategy to address the instruction and readiness issues the student from Cyber Centre for Excellence faced. According to General Paul Stanton, they must complete a variety of follow-on courses to get certified to execute operations (Pomerleau, 2022). This approach aims at reducing the gap between theory and practice by making sure graduates are ready on day one to conduct their missions. Theirs readiness to conduct tasks and operations should be as effective as their theoretical acknowledge are and must be bring closer readiness of all type of soldier (air, ground, space, cyber; navy).

Another way to furnish a skilful and ready workforce in cyberspace is to enhance virtuous competition through practical testing. For instance, EU Member States go through cybersecurity competitions to raise awareness, prepare and train young skilled people, in the hope they turn into future military personnel. Those competitions that mostly take place within the European Network and Information Security Argent (ENISA) allow member states to select cyber talent and train them. Such an approach has collateral benefits, as it gives them the possibility to have a return on investment. Indeed, it impacts their overall cyber security ecosystem by producing skilled individuals that soon will garnish a talent pool transformed in efficient cyber security workforce (Yamin, M.M., Erdodi, L., Torseth, E., Katt, B.. Selecting and Training Young Cyber Talent: A Recurrent European Cyber Security Challenge Case Study. In: Schmorrow, D.D., Fidopiastis, C.M. (eds), 2022). The French DEFNET 2022 exercise conducted in March showed another example of how large-scale training multi-disciplinary level exercise can help to maintain a high level of expertise in cyber defence while strengthening cooperation between multiple actors (Ministry of Defence, 2022).

Finally, the recent opening of the French Campus Cyber defence last July in Paris shows also a great example of how a structure that melts private and public cybersecurity actors, (IT professional, IT & AI researcher, civil society, military) on the basis of four complementary pillars (operation, innovation, training of state's agents, mobilisation) can be, among others, a talent incubator to provide the Armed forces Ministry with a strongly qualified and skilful future personnel. This proximity between different actors will enhance complementarity, cooperation, and information exchanges. That will allow them to be better trained and prepared.

Cooperation and partnership: Exportation of know-how, system, and good practices

Another way to (make other) gain skill and acknowledge is to export within it a cooperative approach and send teams and experts to help domestic personnel.

Lots of countries benefited from cybersecurity cooperation. For example, since May, 28 « Hunt forward » operations have been undertaken across the globe in 16 European countries, including, Estonia, Lithuania, Montenegro, North Macedonia and Ukraine (U.S CYBERCOM, 2022). The renewal in U.S cyber defense authorities and policies allows U.S CYBERCOM to develop a new doctrine of « defence forward » to gain an advantage on adversaries and get first into their structures and networks. First formalised in the DoD cyber strategy in October 2018, this policy aims to work on foreign networks to prevent attacks before they happen and allow DoD to work with partner nations and execute operations in their country, as they currently do in Ukraine. It took place within the « permanent engagement strategy » (Pomerleau, 2019). This hunt forward » doctrine allows to act faster and respond quicker to activities in cyberspace (Pomerleau, 2018). By exporting it, the U.S.A were able to export abroad its know-how, doctrine and technical expertise to train and educate foreign army's personnel on the ground and help civil and military services and structure. This for instance helped Ukrainian forces to harden their network and structures within a cooperation framework (Johnson, 2019).. In Lithuania, CYBERCOM dispatched a cyber team to expose malign activity and strengthen the country's networks amid mounting Russian aggression.

Especially in Ukraine, the USAID program helped the state to strengthen its cyber range capabilities (USAID, 2022). Through this partnership, the U.S planned to give Ukraine structures, substantial training, awareness and acknowledgement. It targeted various actors (electricity facilities, energy regulatory agencies, governmental and citizen-centred commission and structure for elections, action commissioners, civil society, members of Parliament, IT professionals) to train them on how to improve organisational structure and operations, developing strategies and cyber-hardening their networks to address cybersecurity risks.

On an EU level, the current cyber warfare that comes with kinetic warfare Ukraine must face could be an opportunity to implement the EDA-Ukraine MoD (Ministry of Defence) agreement's second point, allowing the MoD to participate in EDA's projects. The Cyber Ranges Federation project under the European Defense Agency umbrella, could be a relevant program. It aims to pool and share existing cyber ranges capabilities between the Member States, contributing to interoperability and by developing a sophisticated and powerful platform at the European level, interconnecting member states' national cyber defence communities.

Bibliography

Audition, à huis clos de M. Stéphane Bouillon, Secrétaire général de la défense et de la sécurité nationale (Juillet 2022), Compte rendu Commission de la défense nationale et des forces armées, Assemblée nationale, pp.2-13, 17 pages, https://www.assemblee-nationale.fr/dyn/16/comptes-rendus/cion_def/l16cion_def2122005_compte-rendu.pdf

Cone, B.D., Thompson, M.F., Irvine, C.E., Nguyen, T.D. (2006), « Cyber Security Training and Awareness Through Game Play », in Fischer-Hübner, S., Rannenberg, K., Yngström, L., Lindskog, S. (eds) Security and Privacy in Dynamic Environments. SEC 2006. IFIP International Federation for Information Processing, vol 201. Springer, Boston ,pp 431–436, https://doi.org/10.1007/0-387-33406-8_37

European Army Interoperability Centre (2018), « Army Cyber Training and Education within Finabel Member States », Focused Questions, pp.1-10, 4 pages, http://finabel.org/wp-content/uploads/2019/01/FQ_Cyber_Training_and_Education_Web2.pdfout

European Parliament Think tank (21 June 2022), Briefing « Russia's war on Ukraine: Timeline of cyber-attacks », pp.1-7, 7 pages, https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/733549/EPRS_BRI(2022)733549_EN.pdf

French Ministry of Defense (11 March 2022), Press corner, https://www.defense.gouv.fr/ema/actualites/sentrainer-au-cyber-combat-defnet-2022 .

International Communication Union, (2020), « Global Cybersecurity Index », ITU Publications, pp.17-21, 172 pages, https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf

Jaspreet Gill, (16 August 2022), « Learning from Ukraine, Army cyber schoolhouse focuses on electromagnetic spectrum", Breaking Defense, 1 pages, https://breakingdefense.com/2022/08/learning-from-ukraine-army-cyber-schoolhouse-focuses-on-electromagnetic-spectrum/

James Pearson, Raphael Satter, Christopher Bing, (12 March 2022), « U.S. spy agency probes sabotage of satellite internet during Russian invasion, sources say », Reuters, 2 pages, https://www.reuters.com/world/europe/exclusive-us-spy-agency-probes-sabotage-satellite-internet-during-russian-2022-03-11/

James.A Lewis, (June 2022) « Cyber War and Ukraine », Center for Strategic and International Studies (CSIS), pp.1-2, 14 pages. https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/220616_Lewis_Cyber_War.pdf?S.iEKeom79InugnYWlcZL4r3Ljuq.ash

Lamar Johnson, (5April 2022), « CYBERCOM Sent a ‘Hunt Forward’ Team to Help Ukraine Harden Systems », MeriTalk, 1 pages, https://www.meritalk.com/articles/cybercom-sent-a-hunt-forward-team-to-help-ukraine-harden-systems/

Mark Pomerleau, (27 November 2018), « Defense officials taking advantage of new cyber authorities », C4ISRNET, 1 page, https://www.c4isrnet.com/dod/cybercom/2018/11/27/defense-officials-taking-advantage-of-new-cyber-authorities/

Bibliography

Mark Pomerleau, (2019), « Two years in, how has a new strategy changed cyber operations ? », C4ISRNET, 1 page, https://www.c4isrnet.com/dod/2019/11/11/two-years-in-how-has-a-new-strategy-changed-cyber-operations/

Mark Pomerleau, (25 August 2021), « New Army cyber school leader wants to fix a problem for graduates », C4ISRNET, 1 page, https://www.c4isrnet.com/smr/technet-augusta/2021/08/25/new-army-cyber-school-leader-wants-to-fix-a-problem-for-graduates/

Pascale Davies, (19 August 2022), « Estonia hit by 'most extensive' cyberattack since 2007 amid tensions with Russia over Ukraine war », Euronew.next, https://www.euronews.com/next/2022/08/18/estonia-hit-by-most-extensive-cyberattack-since-2007-amid-tensions-with-russia-over-ukrain

USAID, Cybersecurity Fact Sheet, 2022, https://www.usaid.gov/ukraine/news-information/fact-sheets/cybersecurity .

U.S CYBER Command Public Affairs, (4 May 2022), News release, https://www.cybercom.mil/Media/News/Article/3020430/us-conducts-first-hunt-forward-operation-in-lithuania/

Yamin, M.M., Erdodi, L., Torseth, E., Katt, B. (2022). « Selecting and Training Young Cyber Talent: A Recurrent European Cyber Security Challenge Case Study », in Schmorrow, D.D., Fidopiastis, C.M. (eds) Augmented Cognition. HCII 2022. Lecture Notes in Computer Science, vol 13310. Springer, Cham, https://doi-org.passerelle.univ-rennes1.fr/10.1007/978-3-031-05457-0_24à .