Cyber warfare has changed the battlefield dramatically. By now, we are all aware that the cyberspace comes with a whole new range of challenges for security and defence, even if we do not fully understand the implications yet. These challenges are not limited to the military domain. Quite the opposite, civilians – individuals, companies, and organizations alike – are often the (soft) target these days. This presents a major challenge as to how to keep people and data safe. NATO and the EU both have a major role to play in this.

On the other hand, there is also a positive dimension to cyber warfare. A variety of digital (big data) tools – apps are being used nowadays by NATO armed forces, allowing for decision-making based on (near) real-time information.

Contents:
Cyber Warfare: The Main Challenge of the Digital Age
Ms. Andreja Friškovec provides a brief historic overview of the development of the cyber domain and its implications for warfare in the 21st century.
EU-NATO Cyber Cooperation: Who Steps in During a Crisis?
Mr. Tommaso de Zan takes a closer look at the ways in which the EU and NATO could respond to a cyber crisis, noting that they each seem to prepare for a different type of crisis. A division of labor is naturally developing, but this then demands a close level of cooperation and mutual consultation.
Cyber Warfare as the Main Challenge in the Digital Age

By Andreja Friškovec

Cyber warfare is one of the main security challenges of the 21st century, if not the biggest challenge. It will without doubt define the next generation of conflict, and according to some, all future wars will start off as cyber wars, or at least have a cyber component to them. Thus, despite being a relatively new domain of warfare, it can be stated with certainty that cyber warfare is here to stay. With the ever increasing role of digital technology in our societies, its role in geopolitics also continues to grow. Cyber warfare, through cyber attacks, but also through online disinformation campaigns, can have a major impact on society. We have seen this recently in the alleged Russian meddling in the U.S. and French elections, and can be sure to see more of it in the future.

The Rise of Cyber Warfare

The history of the internet dates back to the late sixties of the 20th century. The University of California, Los Angeles (UCLA) introduced the public to the internet in a press release on July 3, 1969. It was first used as a communications tool by the U.S. Department of Defense, but became available to the public in the eighties. The first website came online in 1991. Nowadays, it is hard to imagine life without digital access anymore. By 2014, there were more than 1 billion websites and 3 billion active internet users, and the use and applications keep expanding everyday. Cyberspace has grown exponentially, and so has its influence on daily life. That comes with enormous benefits, but also with ever greater risks. In the past few years, the world has seen a number of major cyber attacks, ranging from attacks on military systems and critical infrastructure, such as in Estonia in 2007, to attacks aimed at civilian structures, such as the attack on the NHS in the UK in 2017. The possibilities for doing harm in the cyber realm are as large as they are in “real life”; cyber-espionage, cybersabotage, and plain old hacking are but a few. Despite the fact that large-scale cyber attacks have been around for quite some time now, it was not until 2011 that the U.S. Secretary of Defense declared cyberspace as an operational domain for purposes of organizing, training, and equipping U.S. forces. NATO finally
followed this example in 2016, designating cyberspace an official operational domain of warfare, alongside land, air, and sea. However, in 2014 it was already decided that a major cyber attack could potentially trigger an Article 5 response from the Alliance.

**Challenges and Opportunities**

Cyber warfare is an increasingly popular tool among those who want to inflict harm on others. Cyber attacks are hard to detect, can be carried out from pretty much anywhere – the internet is borderless – and are relatively cheap, as compared to conventional warfare requiring expensive weapons systems. Better yet, even when the attack is detected, attribution is much more difficult than in the event of a conventional attack, making it a favorite for covert involvement, when it must remain possible to deny involvement. Without attribution, there is no accountability, and therefore also no punishment for the perpetrator. Although, it has to be said that great progress in being made in the field of detection and recognition, so things might change.

However, not all is negative in terms of the impact of digital technologies on warfare. Digital technology – and apps – can have an important and positive role to play in modern warfare. A very big difference between the U.S. mission in Iraq in 2007 and that in 2017 is in the big data tools that the soldiers carry with them, helping them to detect and defeat IEDs, among other things. These “apps” often take the form of data analysis and visualization tools that help deployed forces instantly access information about their surroundings.

**Conclusion**

It can be stated without a doubt that cyber warfare is here to stay and requires a response, both from military and civilian structures. As cyberspace is still developing, we are just witnessing the beginning of the potential threats facing us in that domain. However, the same applies to the possibilities that cyberspace has to offer, also in the ways that modern warfare is conducted.

---

**About the author**

Andreja Friškovec is a Law student from Slovenia with an interest in International Criminal Law and security-related topics. She is a remote volunteer for the Coalition for the International Criminal Court, and hopes to pursue a career in international relations.

**Bibliography**


Who invented the Internet?: [https://www.computerhope.com/issues/ch001016.htm](https://www.computerhope.com/issues/ch001016.htm)


Cyber War: [https://www.weforum.org/agenda/2017/01/cyber-war/](https://www.weforum.org/agenda/2017/01/cyber-war/)


Atlantic Voices, Volume 7, Issue 09
EU-NATO Cyber Cooperation: Who Steps in During a Crisis?

By Tommaso de Zan

In May 2017, a ransomware dubbed WannaCry spread across the world and infected over 230,000 systems in more than 150 countries. Victims of the malicious software were asked to pay a ransom of $300 and the hackers behind the attack collected a total of $77,000 in payments. A month later, a different computer virus wreaked even more havoc. Initially targeting some Ukrainian organizations, the wiper NonPetya quickly infected systems across Europe and hit businesses and critical infrastructures alike. According to the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), the two malwares ‘call for a joint response’. But from whom, precisely? In Europe, many of the countries affected by the two viruses were EU and NATO members. In the past, both organizations have developed policies to thwart attacks against the confidentiality, authenticity, integrity and availability of their computer systems, networks and data. In fact, in June 2016, NATO Secretary General Jens Stoltenberg declared that ‘a severe cyber-attack may be classified as a case for the alliance. Then NATO can and must react.’ Similarly, a month later, the European Commission (EC) wrote that ‘the EU needs to prepare itself for the possibility of a large-scale cyber crisis, including, for instance, simultaneous attacks on critical information systems in several member states’. Moreover, attacks by WannaCry and NonPetya occurred after the Council of the EU and the North Atlantic Council (NAC) endorsed a set of common proposals to deepen cooperation in crisis response and cybersecurity/defense. This raises the question: which organization will step in during a “cyber crisis”?

NATO and EU Cyber Policies and Crisis Management

NATO and EU cyber policies provide a good starting point to understand the organizations’ overall posture on cybersecurity crisis management. Although being concerned with cyber defense well before, NATO approved its first cyber defense policy in 2007, after DDoS attacks against Estonia paralyzed the Eastern European country for nearly two weeks, and the Russia-Georgia war in 2008 brought forth the realization that cyber operations were quickly becoming a major component of modern warfare. Today, NATO cyber defense policy is articulated in two principles and two main priorities.

Regarding the principles, the Alliance stated that existing regimes of international law apply to cyberspace and that cyber defense is part of the Alliance’s core task of collective defense. At the Wales Summit in 2014, the Heads of States and Governments declared that an Ally can invoke Article 5 of the Washington Treaty (collective self-defense) should a cyber-attack have a comparable effect to that of a conventional armed attack. To operationalize that, at the Warsaw Summit in July 2016, policymakers recognized cyberspace as a domain of operations in which NATO must defend itself as it does in the air, land, and at sea.

Besides these two main principles, NATO also made clear to pursue two principal priorities. The first is to defend its own systems and networks, including
those deployed in missions and operations. This implies that the protection of member states’ information systems is primarily their own responsibility. Indeed, the 2016 Cyber Defence Pledge confirms Allies’ ‘national responsibility […] to enhance the cyber defenses of national infrastructures and networks’. The second priority is to encourage allies to develop their own cyber defense capabilities and to assist them on a case by case basis. In the case of a significant attack on the networks of an Ally, NATO will assist the affected country, and facilitate its recovery. This will be enabled by a Memoranda of Understanding between member states’ national defense authorities and the NATO Cyber Defence Management Board. If such a situation occurs, any Ally – particularly those lacking cyber defense capabilities – could receive assistance from the Rapid Reaction Team (RTT) of the NATO Computer Incident Response Capability (NCIRC), following approval by the NAC.

In July 2016, the EU adopted the first EU-wide legislation on cybersecurity, the so-called Directive ‘concerning measures for a high common level of security of networks and information systems across the Union’. The Directive helps to clarify the broader framework in which cyber incidents in the EU are managed. First, it clearly specifies the entities to be monitored by national authorities. It states: ‘to cover all relevant incidents and risks, the Directive should apply to both operators of essential services and digital service providers’. Essential service providers belong to sectors such as energy, transport, banking, financial market infrastructure, health, drinking water supply and distribution, and digital infrastructure, whereas digital services refer to online marketplaces, online search engines and cloud computing services. Second, it creates the Computer Security Incident Response Team’s (CSIRT) network, comprised of national member states’ CSIRTs and the CERT-EU to coordinate a response to national and cross-border incidents. In September 2017, the EC published the “Recommendation on Coordinated Response to Large Scale Cybersecurity Incidents and Crises”, which defines such crises as ‘incidents which cause disruption too extensive for a concerned Member State to handle on its own or which affect two or more Member States or EU Institutions with such a wide-ranging and significant impact of technical or political significance that they require timely policy coordination and response at Union political level.’ The recommendation, in the form of a Blueprint, assigns roles to the various EU and national actors involved in a potential crisis and outlines a three-level approach (tactical, operational and political) to address a potential crisis. The Blueprint is the first attempt to integrate cyber elements in the framework of the Integrated Political Crisis Response (IPCR), which is a crisis management mechanism providing the Presidency of the Council with an instrument for political coordination between member states in case of crisis. The recommendation also indicates that the European External Action Service’s (EEAS) Crisis Response Mechanism will be activated, should the crisis have an important external or Common Security Defence Policy (CSDP) component, and suggests that cooperation at the political level might require coordination with the UN, the OSCE and “particularly NATO,” although it does not elaborate much on the collaboration with the Alliance.

Recently, the EU and NATO agreed to deepen cooperation in cyber defense/security. In February 2016, the IT security response teams of the two organizations, NATO’s NCIRC and the EU’s CERT-EU, signed a technical arrangement to facilitate the
sharing of technical unclassified data. This was the prelude to deeper cooperation later in the year. At the Warsaw Summit in July 2016, the two organizations opted to expand their cooperation in crisis response and cyber security/defense, and concretized it in December 2016 through a set of common proposals. On crisis management, the two institutions vowed to synchronize their crisis response mechanisms, namely EU’s IPCR and NATO’s Crisis Response System. On cyber security/defense, the two organizations pledged to consult each other on ways to integrate cyber defense into mission planning and execution, strengthening training, fostering research and innovation, and cooperating in cyber exercises.

Whilst illustrative, the EU’s and NATO’s cyber policies lack the needed granularity to comprehend what kind of “crisis” they are preparing for, and how. To do that, analyzing the EU’s and NATO’s cyber exercises, namely Cyber Europe and Cyber Coalition, is a step further in the direction of achieving a more complex level of understanding. Indeed, EU Cyber Europe exercises are ‘simulations of large-scale cybersecurity incidents that escalate to become a cyber crisis’, featuring scenarios that are inspired by real life events. Likewise, NATO Cyber Coalition exercises ‘test and train cyber defenders to respond to cyber challenges through realistic defensive exercises’.

**Cyber Coalition and Cyber Europe**

NATO’s Cyber Coalition exercise has been taking place every year since 2008. Even though data has become increasingly scant, publicly available information on exercises between 2008 and 2016 reveal that scenarios have been mainly centered around the protection of NATO’s networks, including hackers targeting the Alliance’s soldiers during its own cyber games, SCADA systems, the AWACS system, officers’ smart watches during secret meetings, and radars’ targeting capabilities. Interestingly, vague references to scenarios on the protection of member states’ (likely military and defense) systems can be found in the public domain. Nonetheless, it is impossible to assess whether these scenarios foresaw breaches that prompted the Alliance to assist Allies through the RRT or scenarios deriving from cyber-attacks with consequences comparable to an armed attack.

The most detailed account of NATO Cyber Coalition exercises is the cyber game in 2014. In this exercise, a team of around 100 foreign soldiers and intelligence officials trenched in Estonian forests near Tartu (where the Alliance cyber range is located) began launching sophisticated hacking campaigns against NATO’s teams in Europe and North America. Troops’ phones were hacked after a malicious application was downloaded, following which hostile intelligence officers gained access to the coalition’s networks. Other threat scenarios were then injected into the cyber game: a supplier of military equipment had its manufacturing process compromised; attackers gained control of the system governing NATO’s AWACS surveillance aircraft; and a senior military officer was blackmailed into dumping some of the Alliance’s classified information.

Cyber Europe exercises began in 2010 and, thus far, four exercises have been organized every other year. Although the details of the latest 2016 exercise were not divulged, information on European exercises are usually ampler. Unsurprisingly, EU scenarios are largely based on attacks against operators of essential services and digital service providers, hence the physical and digital infrastructures that are listed in the NIS directive.
Coincidentally, the exercise with the broader available evidence took place in 2014 as well. In this cyber game, EU institutions were subject to attacks that attempted to gather information on a fictitious regulation that would tax the development of green technologies. Disinformation campaigns and operations aimed at exfiltrating data and at destabilizing the market were carried out. Other incidents involved malware infecting mobile devices, DDoS and advanced persistent threats. These attacks notwithstanding, the scenario saw the regulation pass and the attacks escalate with zero-days exploiting vulnerabilities in critical infrastructures and online services, during a cold winter and to an increasingly preoccupied population.

These scenarios certainly provide a more sophisticated level of understanding, but analyzing how NATO and the EU behave in actual crises would provide the definitive piece of evidence to answer the puzzle delineated in the introduction. In this regard, the recent outbursts of WannaCry and NonPetya are significant episodes in the two organizations’ conceptualization of a “cyber crisis” and their crisis management procedures.

**WannaCry and NonPetya**

In May 2017, the WannaCry pandemic propagated with unusual speed across thousands of systems worldwide, including in Europe. Critical infrastructure operators such as health, energy, transport, finance, and telecom were also affected. To cope with the ransomware, a dedicated task force was established at the EU Agency for Network and Information Security (ENISA) to coordinate regional action. According to the Agency, it was the ‘first ever case of cyber cooperation at the EU level’ in which EU Standard Operating Procedures, established in February 2014, and usually rehearsed during Cyber Europe exercises, were followed to handle the crisis.

The EU cooperation mechanism was tested for the second time two months later with the NonPetya outbreak. The wiper used tax and accounting software packages to gain a foothold in corporate networks, and to subsequently spread to 60 countries, though mainly in Europe. According to ENISA, the CSIRTs network was paramount in enhancing a cross-border information flow, and a better understanding of mitigation procedures, as well as reduced delays in incident responses at the national level.

From publicly available sources, it is not known whether NATO activated any sort of coping mechanism during the spread of the two malwares. Nonetheless, Secretary General Stoltenberg stated that the CERT-EU and NCIRC exchanged information and warnings in real-time during the response phase of WannaCry.

**Division of Labor and “Crisis” Ambiguity**

By combining the analyses of EU and NATO cyber policies, exercises and responses to recent relevant episodes such as WannaCry and NonPetya, there seems to be quite a distinct division of labor between the two organizations. While the EU seems to prepare itself for crises mostly affecting its member states’ critical infrastructures, NATO mainly trains its personnel to thwart operations against its own networks and, when conditions are met, to assist Allies when their military and defense networks and systems are under attack.

The recent WannaCry and NonPetya crises triggered the cooperative mechanism of the EU, but clearly did not prompt the NAC to authorize any collective response or, so it seems, the deployment of NCIRC’s RRT. What both organizations did was to exchange information and warnings in real-time – per the agreement in the cyber security/defense cooperation proposals from December 2016. In sum, the handling of the WannaCry and NonPetya crises seems well-aligned with what the two organizations have been preparing for.
in their exercises, as well as what they have stated as their official policies.

Based on the above, the answer to the question posed in the introduction on who will intervene during a cyber crisis seems to lie in the ambiguity of the word “crisis” and the different meanings it bears in EU and NATO’s policies. In official EU documents, words such as cyber “incident”, “attacks”, and “crisis”, coupled with connotations such as “large-scale”, “massive”, or “major” are often used in similar contexts, also when describing exercises in which member states practice. Within NATO, however, the term “cyber crisis” is rarely (if ever) used, as opposed to softer terms such as “cyber incidents”. And when referring to “significant cyber-attacks”, official documents, especially the more recent ones, seem to denote cyber operations as those expected to cause injury/death or to inflict damage/destruction on objects. This is why the same CCDCOE, which called for a joint response during the NonPetya campaign, suggested that the absence of effects comparable to that of an armed attack meant that collective defense by NATO was not a viable option and, instead, proposed an investigation on a global level.

**Conclusions**

Despite the ambiguity of the word crisis, the analysis shows a de facto division of labor between the EU and NATO in dealing with cyber incidents potentially escalating to a “crisis”. The EU appears to primarily focus its efforts on the protection of critical civilian infrastructures listed in the NIS Directive through the CSIRT network; NATO seems mainly concerned about preventing successful attacks against its own networks, assisting member states suffering significant attacks against their military and defense systems, and in case of cyber operations with effects comparable to an armed attack, triggering the Alliance’s collective response. This does not mean, however, that the way that the EU and NATO would handle a crisis is a settled issue.

So far, this division of labor has been possible because few digital attacks have produced kinetic effects. Such attacks have not come nearly as close to causing the same kind of physical damage as, for example, tank strikes. Nonetheless, this could change in future scenarios when more sophisticated cyber operations would intertwine the two distinct “domains” (the civilian/critical infrastructure and the defense/military networks) in which the two organizations now seem to operate. For instance, what would happen if a foreign cyber operation against a critical infrastructure of an EU and NATO member state produced an effect comparable to that of an armed attack? How would deconfliction occur between EU and NATO? Currently, how the EU’s IPCR or EEAS’s Crisis Response System would coordinate with NATO’s Crisis Response system is still hard to foresee.

As seen above in the section on EU and NATO policies, practical policy measures have recently been introduced to divert potentially conflicting scenarios. Further development of the Blueprint on crisis coordination and its formal adoption by member states could be of help, especially if it will expand on possible coordination measures at the political level between the EU and NATO, a topic which is treated only marginally in the current proposed scheme. Moreover, the newly agreed common actions on cybersecurity and crisis management, which recognize the importance of making participation in the EU’s and NATO’s exercises possible, might dispel some of the doubts on how the two organization operate.

In spite of such practical steps, the answer to these questions posed above is inevitably linked to the more profound challenge of the future of the EU as a possible
“security and defense union” and its relationship with NATO. Some authors have already argued that the Mutual Defence Clause (Art. 42 TEU), which is interpreted as an equivalent of NATO’s Article 5, could be invoked by an EU member state if a cyber-attack qualifies as armed aggression. At the same time, in a reflection paper on the future of European Defence published in June 2017, the EC envisioned a scenario in which the protection of Europe would become a mutual responsibility between the EU and NATO, and that the EU ‘would coordinate response scenarios and actions in case of cyber-attacks’, and would be able ‘to deploy detection and offensive cyber capabilities’. Although this possibility seems quite remote for now, even incremental steps by EU member states towards a deeper defense union should propel the two organizations to readily deconflict their respective mitigation mechanisms and procedures. Regardless of the obvious challenges that this would imply, in a time of increasing perils stemming from conventional and unconventional threats, a swift and effective collaboration between EU and NATO will remain the key to the security of EU citizens.

**About the author**

Tommaso de Zan is a PhD student in Cyber Security at the University of Oxford, where he analyses policies aimed at reducing the cyber security skills shortage. Previously, he was an Associate Fellow at the European Union Institute for Security Studies (EUISS) in Brussels and a Researcher at the International Affairs Institute (IAI) in Rome. He holds a Master’s degree in International Relations from the University of Bologna (Forlì) and was an exchange student at the University of Denver and Université catholique de Louvain.

**Bibliography**

Adelina Campos de Carvalho, NATO’s Cyber Defenders: Hacking, a way of life, NCIA, 1 October 2017, https://www.ncia.nato.int/NewsRoom/Pages/170110-Hack-for-Living.aspx


EEAS, EU and NATO increase information sharing on cyber incidents, 10 February 2016, https://eeas.europa.eu/headquarters/headquarters-homepage/5254_en


Andy Greenberg, Petya ransomware epidemic may be spillover from cyberwar, Wired, 6 June 2017, https://www.wired.com/story/petya-spillover-from-cyberwar

Sam Jones, NATO holds largest cyber war games, Financial Times, 20 November 2014, https://www.ft.com/content/9c46a600-70c5-11e4-8113-001144feabdc0?mhq5j=e6


SHAPE NATO, NATO's largest cyber defence exercise: Cyber Coalition 16, 8 December 2016, https://www.youtube.com/watch?v=og9YxZydRow


US Military Videos By OpsLens, Cyber Coalition Exercise, 28 January 2014, https://www.youtube.com/watch?v=beWiQweeU1E
YATA/ATA Programs

New YATA Chapters
We are very excited to announce that the YATA family was recently expanded with two new chapters, YATA Canada and YATA US have recently been start up, both already having hosted their first events too.

Give them a warm welcome by giving them a like on Facebook and following them on Twitter, to never miss an update on their activities!

YATA Canada
Youth chapter of the
NATO Association of Canada
Facebook: @yatacanada
Twitter: @yatacanada

YATA US
Youth organization of the
Atlantic Council
Facebook: @YATAUS
Twitter: @YATA_US

Atlantic Voices is always seeking new material. If you are a young researcher, a subject expert or a professional and feel you have a valuable contribution to make to the debate, then please get in touch. We are looking for papers, essays, and book reviews on issues of importance to the NATO Alliance. For details of how to submit your work please see our website at: http://atahq.org/atlantic-voices/

Editor: Marianne Copier

Images should not be reproduced without permission from sources listed, and remain the sole property of those sources. Unless otherwise stated, all images are the property of NATO.