Wilfried
Martens Centre
for European Studies

Cyber-Defence IN FOCUS

Strengthening the EU's Resilience in the Virtual Domain

August 2017

Executive summary

Gonçalo Carriço

This paper analyses the unstoppable phenomenon of globalisation through the lens of cyberspace. It looks at how the threats associated with this domain could evolve into a cyberwar. The paper assesses the EU's stance on cyberspace and elaborates the directions that the EU should develop and pursue in this regard. It begins by examining the meaning of various cyber-related terms as a way of explaining the risks, threats and challenges of cyberspace. It then goes on to detail the EU's approach to cyberspace. The paper concludes by outlining a way to increase the EU's cyber-defence capacity and scope through the creation of an EU cyber-command that would centrally coordinate operational capacity in cyberspace in order to pursue the development of hard and offensive cyber-power. Finally, the paper also builds on the European People's Party's (EPP's) call for strengthened resilience against cyberwar and offers a suggestion for an EU response to hybrid warfare and cyberwar, as outlined in the EPP's Congress document *Europe Secures Our Future.*[1]

Keywords Cyberwar – Cyberwarfare – Cybersecurity – Cyber-threat – European Union

[1] EPP, *Europe Secures Our Future,* document adopted at the EPP Congress, Malta, 29–30 March 2017, accessed at http://www.epp.eu/papers/congress-document-europe-secures-our-future/ on 17 July 2017.

Introduction

With our ever-growing dependency on cyberspace, our vulnerability is increasing exponentially. Cyberspace is becoming a space for both good and evil. But what exactly is cyberspace, and how is it being used for cyberwar?

Cyberspace is generally associated with the online world of computer networks, and especially with the Internet, the borderless nature of which is its main characteristic. As the 2015 *Security Strategy of the Czech Republic* put it, cyberspace is an 'environment that has no geographic borders and in which the distance between the source of threat and the potential target becomes relative'.[2] Unlike the other domains of war (sea, land, air and space), the anonymity and unpredictability of cyberspace—over and above the absence of borders—make it a complex threat environment and the ideal field for warfare.

In addition, the target of a cyber-attack may have no notion (physical or virtual) of being attacked, or even whether the attack is happening or has happened. It is also difficult to discern the nature of a cyber-attack and its perpetrator. In civil/military terms, therefore, and according to the *Tallinn Manual on the International Law Applicable to Cyber Operations*, a cyber-attack 'is a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects'.[3] In fact, NATO has identified cyberspace as the fifth domain of war, a domain which must be defended as effectively as those of air, land and sea.

[2] Ministry of Defence & Armed Forces of the Czech Republic, *Security Strategy of the Czech Republic* (Prague, 2015), 13, accessed at http://www.army.cz/images/id_8001_9000/8503/15_02_Security_Strategy_2015.pdf on 17 July 2017.

[3] M. N. Schmitt (ed.), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge: Cambridge University Press, 2017), 106, accessed at https://books.google.be/books/about/Tallinn_Manual_2_0_on_the_International.html?id=n9wcDgAAQBAJ&printsec=frontcover&source=kp_read_button&redir_esc=y#v=onepage&q&f=false on 17 July 2017.

Threats and challenges

Consider the following examples: the 2007 Distributed Denial-of-Service (DDoS)[4] attack against Estonian government networks, the 2008 attacks on Georgia's government communications, and the 2012 involvement by a senior US official, though unacknowledged officially, in deploying Stuxnet and Flame (and possibly Duqu and Gauss) against a network controlling Iranian nuclear centrifuges, as well as against other Middle Eastern networks.[5] In addition there was the 2012 DDoS attack against US financial institution networks, likely carried out under the direction of a nation state based on intentional and targeted selection, and the recent cyber-attacks on Ukraine's critical energy infrastructure, namely the Prykarpattiaoblenergo (power grid), which affected 700,000 households,[6] and the Boryspil airport networks.[7] The latter attacks were supposedly sponsored by Russia and linked to the conflict in Crimea—thus making Ukraine the Russians' test lab for cyberwar. All these examples have shown a real capacity to destroy or damage physical property—or to significantly damage the economy and society if carried out over a long period of time—thus representing a strategic shift in focus. This makes it clear that some states have addressed the development of cyber-defence and cyber-offence capabilities in order to be prepared for a possible 'cyberwar', taking into account the global economy's ever-growing dependence on public infrastructure and on the importance of secure access to, and the stability of, cyberspace.

Another strand of cyber-attacks with a high impact on our societies is those being carried out to undermine trust in liberal democracy. Cases such as the attempt to hack the Konrad-Adenauer-Stiftung, a German foundation linked to Chancellor Angela Merkel; the hacking of Demo-

[4] A DDoS is a malicious attempt from multiple systems to make computer or network resources unavailable to their intended users, usually by interrupting or suspending services connected to the Internet. *Incapsula,* 'Denial of Service Attacks', accessed at http://www.incapsula.com/ddos/ddos-attacks/denial-of-service on 17 July 2017.

[5] E. Nakashima, G. Miller and J. Tate, 'U.S., Israel Developed Flame Computer Virus to Slow Iranian Nuclear Efforts, Officials Say', *The Washington Post,* 19 June 2012, accessed at https://www.washingtonpost.com/world/national-security/us-israel-developed-computer-virus-to-slow-iranian-nuclear-efforts-officials-say/2012/06/19/gJQA6xBPoV_story.html on 17 July 2017.

[6] *Frankfurter Allgemeine Sonntagszeitung,* 'Hacker verursachten Stromausfall: Erkenntnisse über einen Cyberangriff in der Ukraine', 10 January 2016.

[7] P. Paganini, 'Ukraine Blames Russia of Cyber Attacks Against the Boryspil Airport', *Cyber Defense Magazine,* accessed at http://www.cyberdefensemagazine.com/ukraine-blames-russia-of-cyber-attacks-against-the-boryspil-airport/ on 9 July 2016.

cratic Party emails during the 2016 US Presidential election; the attack on Merkel's Christian Democratic Union (Christlich Demokratische Union Deutschlands); the hack of the French broadcaster TV5 Monde; the recent attack on French President Emmanuel Macron's 2017 campaign; and the widespread dissemination of propaganda and fake news are examples of this. Cyber-attacks are also being used for geopolitical ends, as in the Gulf, where an attack has sparked a major political crisis. Such instances provide strong reasons for concern and action.

Concerning the 2007 cyber-attack in Estonia that Russia officially denied being involved in, an appeal for help to the EU and NATO was made by Estonian officials on the grounds that what happened should be viewed as an act of war in the digital era. The EU and NATO countered that a cyber-attack did not constitute military action; however, Estonia's vulnerability to cyber-threats has opened the door for a discussion of what constitutes an act of war in the digital age.

The EU's approach to cyberspace

In February 2013, the European Commission and the High Representative of the Union for Foreign Affairs and Security Policy (High Representative) Federica Mogherini put forward the EU's vision in this domain in order to clarify roles and responsibilities and to set out the actions required, based on strong and effective protection and the promotion of citizens' rights, to make the EU's online environment open, safe and secure. The strategy, entitled *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace* intends to counter both breaches of cybersecurity on critical infrastructure, as well as cybercrime against the private sector and individuals. It also seeks to promote freedom and ensure respect for fundamental rights online—based on the idea that the EU's core values should apply equally in the digital and physical realms. The strategy has five priorities:

1. achieving cyber-resilience,

2. drastically reducing cybercrime,

3. developing cyber-defence policy and capabilities related to the Common Security and Defence Policy (CSDP),
4. developing the industrial and technological resources for cybersecurity, and
5. establishing a coherent international cyberspace policy for the EU and promoting core EU values.[8]

The Network and Information Security (NIS) Directive accompanies the strategy and, among other things, it sets a mandatory reporting standard for significant cyber-incidents across all critical infrastructure sectors, as well as for providers of key Internet services.[9]

The cybersecurity strategy also underlines the EU's commitment to existing international laws regulating cyberspace, such as the Budapest Convention on Cybercrime, the International Convention on Civil and Political Rights, and the Geneva Convention.

The clarification of roles identified in the strategy—that is, who does what in cyberspace—is divided into categories: cybercrime and justice, cyber-resilience, cyber-diplomacy and cyber-conflicts; and levels: regional, global and EU.

Although all five priorities are interdependent, I will focus primarily on developing the cyber-defence policy and capabilities related to the CSDP. This priority highlights the fact that given the need to 'increase the resilience of the communication and information systems supporting Member States' defence and national security interests, cyber defence capability development should concentrate on detection, response and recovery from sophisticated cyber threats'.[10]

To uphold this priority, the Council of the EU, in its conclusions of November 2013, which recognised the importance of networks in today's globalised world and the need for the EU to engage in all domains—land, air, sea, space and cyberspace—invited the High Representative, the

[8] European Commission, *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace,* Joint Communication, JOIN (2013) 1 final (7 February 2013), accessed at http://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf on 17 July 2017.

[9] European Commission, 'Network and Information Security Directive: Co-Legislators Agree on the First EU-Wide Legislation on Cybersecurity', 9 December 2015, accessed at https://ec.europa.eu/digital-single-market/en/news/network-and-information-security-directive-co-legislators-agree-first-eu-wide-legislation on 17 July 2017.

[10] European Commission, *Cybersecurity Strategy,* 11.

European Defence Agency (EDA) and the Commission to produce an EU Cyber Defence Policy Framework (CDPF) in 2014.

Furthermore, the European Council, in its conclusions on CSDP in December 2013, recognising that new security challenges are emerging and that Europe's internal and external security dimensions are increasingly interlinked, reinforced the call made by the Council of the EU for the Union and its member states to be able to respond to cyberspace challenges in cooperation with NATO efforts.

The EU CDPF was published on 18 November 2014 and laid the groundwork for countering threats arising from cyberspace; it specified five priority areas for CSDP cyber-defence:

1. supporting the development of member states' cyber-defence capabilities related to CSDP;
2. enhancing the protection of the CSDP communication networks used by EU entities;
3. promoting civil–military cooperation and synergies with wider EU cyber-policies, relevant EU institutions and agencies, as well as with the private sector;
4. improving training, education and joint exercise opportunities; and
5. enhancing cooperation with the relevant international partners, particularly NATO.[11]

On the international stage, the EU has the ambition to be a normative global actor, capable of creating an effective and constructive culture of cybersecurity within and beyond the EU by establishing a coherent international cyberspace policy. This will enable it to promote the core EU values of democracy, human rights and the rule of law, including the right to freedom of expression, access to information and the right to privacy—the EU's so-called cyber-diplomacy tenets, as laid down in the *Council Conclusions on Cyber Diplomacy,* adopted by the General Affairs Council on 11 February 2015.[12]

[11] Council of the European Union, *EU Cyber Defence Policy Framework,* 15585/14 (18 November 2014), accessed at http://data.consilium.europa.eu/doc/document/ST-15585-2014-INIT/en/pdf on 17 July 2017.

[12] Council of the European Union, *Council Conclusions on Cyber Diplomacy,* 6122/15 (11 February 2015), accessed at http://data.consilium.europa.eu/doc/document/ST-6122-2015-INIT/en/pdf on 17 July 2017.

More recently, in June 2016, the High Representative presented the Global Strategy for the EU's Foreign and Security Policy. The strategy clearly outlines the importance of increasing the focus on cybersecurity in order to maintain an open, free and safe cyberspace. This will entail

1. strengthening technological capabilities to mitigate threats and increase resilience;

2. fostering innovative information and communication technology systems;

3. weaving 'cyber' issues into all policy areas;

4. reinforcing the 'cyber' elements in CSDP missions;

5. supporting political, operational and technical cyber-cooperation between member states;

6. enhancing cybersecurity cooperation with the US and NATO;

7. developing strong public–private partnerships; and

8. fostering a common cybersecurity culture and preparedness for possible cyber-disruptions and attacks.

Member states should also translate their commitment to mutual assistance and solidarity, as enshrined in the treaties, into action in this field.[13]

The missing element in EU policy in cyberspace

One might interpret the EU's cybersecurity policy as diverging from the policies being developed in the rest of the world concerning the nature of 'cyber-power'. This is because the EU is not developing the kind of hard and offensive cyber-power concepts pursued by other states in accordance with the logic of national security and superiority. Rather, the EU is focusing on soft power—legal and protective—such as capacity-building, to enable detection, response and recovery from sophisticated

[13] EU, *A Global Strategy for the European Union's Foreign and Security Policy* (June 2016), accessed at http://europa.eu/globalstrategy/sites/globalstrategy/files/regions/files/eugs_review_web_0.pdf on 17 July 2017.

cyber-threats. Due to its core norms, competences and values, the EU's approach to cyberspace is more geared towards cybercrime.

The EU's missing element in cyberspace relates, then, to its defence and the civil/military dimension, as the EU's policies and actions are only concerned with and engaged in cyber-self-protection and in assuring access to cyberspace in order to enable its operations and missions. Offensive capabilities are possible, but these would need to be developed or deployed by a member state, not under the EU umbrella.

The EU's cyber-machinery and its instruments

According to the annual report from the Council to the European Parliament on the Common Foreign and Security Policy (CFSP), cyber-defence capabilities still remain critically low in terms of capacity development.[14]

The EDA's main focus in terms of cyber-defence is on training capacity. While this is extremely relevant, we can see that the development of the operational level is being left behind, even though its inclusion is envisaged in the CDPF—for example, in the unified cyber-defence concept for the CSDP that covers military operations and civilian missions.

The European Network and Information Security Agency (ENISA), created in 2004, is the 'centre of expertise for cyber security in Europe. ENISA is contributing to a high level of network and information security (NIS) within the European Union, by developing and promoting a culture of NIS in society to assist in the proper functioning of the internal market'.[15] The recently approved NIS Directive will be the first piece of EU legislation specifically aimed at improving cybersecurity throughout the Union. The NIS Directive in itself represents a very significant step forward in the approach to securing EU information systems, and ENISA has a big role to play in upholding it, in cooperation with the member states.

[14] Council of the European Union, *Draft Annual Report from the High Representative of the European Union for Foreign Affairs and Security Policy to the European Parliament: Main Aspects and Basic Choices of the CFSP,* 11083/15 (20 July 2015), accessed at http://data.consilium.europa.eu/doc/document/ST-11083-2015-INIT/en/pdf on 18 July 2017.

[15] ENISA, 'About ENISA', accessed at https://www.enisa.europa.eu/about-enisa on 17 July 2017.

EUROPOL's European Cybercrime Centre, created in 2013, is the focal point of the EU's fight against cybercrime, contributing to faster response times in the event of cyber-attacks. Its goal is to strengthen the law enforcement response to cybercrime in the EU and to help protect European citizens, businesses and governments.

As well as the EU's agencies that are involved in 'cyber' matters—the EDA, ENISA, the European Cybercrime Centre and the European External Action Service—and its policy frameworks, the EU has also passed three pieces of legislation which are extremely important with regard to cyberspace.

One is the aforementioned NIS Directive, which will provide legal measures to boost the overall level of cybersecurity in the EU by increasing the cybersecurity capabilities of member states, enhancing cooperation and ensuring high standards for risk management practices in key sectors involving critical infrastructure (e.g. energy, transport and banks).

Another is the General Data Protection Regulation, set to enter into force in 2018. This will uphold EU citizens' rights and values (such as privacy) online, just as these rights and values have already been guaranteed offline. Although this legislative measure is not directly related to cybersecurity, it fosters the uptake of protective measures in all online services operations in the EU, whether they are provided by EU companies or not. It also raises the bar on data protection standards, thus increasing the EU's global capacity for cyber-diplomacy related to its core values.

The final legislation comes in the form of Article 222 of the Treaty on the Functioning of the EU and Article 42(7) of the Treaty on EU. The former is called the Solidarity Clause, while the latter is sometimes informally referred to as the Mutual Defence Clause. Their purpose is to strengthen cooperation between member states and the EU institutions in case of a crisis or armed aggression. The Solidarity Clause created an obligation for all member states to act jointly and to assist one another in the event of disasters and crises exceeding their individual response capacities (this clause would have covered the Estonian request to the EU during the 2007 cyber-attack). A set of more detailed implementation guidelines is attached to this clause in order to uphold this provision and provide operational meaning for the concept. Concerning the Mutual

Defence Clause, guidelines for its implementation still need to be defined in order to bring clarity to the rhetorical concept. The EU Cyber Security Strategy addresses the question of whether the Solidarity Clause could be invoked in the case of a major cyber-incident or attack. The EU's CDPF, adopted by the Council in November 2014, clearly states that 'the objectives of cyber defence should be better integrated within the Union's crisis management mechanisms. In order to deal with the effects of a cyber crisis, relevant provisions of the Treaty on the EU and the Treaty on the Functioning of the EU may be applicable, as appropriate'.[16] In any case, neither clause could be activated to deal with a cyber-attack itself, but rather only with its consequences.

Increasing the EU's cyber-defence capacity

The EU, with the support of ENISA, should intensify the promotion of a single market for cybersecurity products (aligned with the Digital Single Market strategy) by fostering research, development and investment. It should foster cooperation at the early stages of the research and innovation process in order to build cybersecurity solutions for various sectors, such as energy, health, transport and finance. This will also help to build a well-established EU market for cybersecurity, one which uses new business models and fosters innovative small and medium-sized enterprises that are able to scale up quickly.

This initiative should find synergies with projects such as the Galileo programme (on satellite data for operations) and the European Open Science Cloud (which encompasses the European Data Infrastructure for deploying high-bandwidth networks, large-scale storage facilities and super-computing capacity) to develop a public–private—civilian–military cyber-ecosystem that would generate the best innovation in the cyber-realm to tackle existing and upcoming cyber-related challenges. It would also enable the exploration of new possibilities in cryptography, as well as in trending technologies, such as Artificial Intelligence (AI)

[16] Council of the European Union, *EU Cyber Defence Policy Framework,* 3.

and blockchain,[17] so that these can contribute to the development of new methods to help identify attackers (cyber-forensics).

In addition, the EU should create a European university able to attract and develop skilled workers beyond those needed for the traditional administrative and functional needs of the EU. The university would teach cyber-military skills in command and control, and also provide the technical training needed for specialists in data science, analysis, cyber-forensics, AI and robotics, all while encompassing an overarching EU mindset. We must keep in mind that today's most developed commodities, such as the Internet, came from the defence sector through strategic investments in research and development and were created in the context of a developed ecosystem. This magic triangle (military–industrial–academic) led Vannevar Bush to highlight in his report immediately after the Second World War that 'it's clear beyond all doubt that basic science—discovering the fundamentals of computer science (among others)—is absolutely essential to national security and crucial for . . . economic security'.[18]

To this end, financial resources and political will are needed. The EU should build on the momentum triggered by the recent terrorist attacks in Paris and Brussels, including the relationship between these attacks and conflict zones outside the EU and vis-à-vis the migration crisis. Momentum has also arisen from the tensions with Russia over the conflict in Ukraine and Russia's deployment of unconventional measures throughout cyberspace to undermine trust in liberal democracies and institutions. Some political leaders have recently stressed, in one way or another, the need for better cooperation and coordination. In a globalised world with challenges, crises and events occurring every hour, there are serious doubts that a nation could 'survive' on its own in a 'catastrophic' situation maintained or started in cyberspace.

Concerning the financial dimension, we should derive as much funding as possible from the myriad of EU funding programmes. From the European Defence Fund to Horizon 2020 (namely the €450 million al-

[17] Blockchain is the technology that enables secure transactions using crypto-currencies (such as Bitcoin) and has the potential to prevent cyber-attacks and increase security by blocking identity theft, preventing data tampering, and stopping denial-of-service attacks.

[18] V. Bush quoted in W. Isaacson, *The Innovators: How a Group of Hackers, Geniuses, and Geeks Created the Digital Revolution* (New York: Simon & Schuster, 2015), 220.

located to the public–private partnership on cybersecurity,[19] expected to trigger €1.8 billion in investments by 2020), and from the Connecting Europe Facility to Galileo and to the financial instruments that support the Digitise European Industry initiative of which the European Cloud is part—all should be considered and applied to in order to develop the data infrastructure discussed above. Such funding should also be used to support the aforementioned university and supportive ecosystem for cyber-start-ups (the equivalent of the 'Silicon Valley of cybersecurity' in the US). In this way, such an environment could attract and retain talent and investment in the European Defence Technological and Industrial Base (and also reduce dependency on external suppliers). In sum, we need to build our digital autonomy from scratch.

In line with the European People's Party's (EPP's) position on the need to create an EU Operational Headquarters[20] as a means to ensure quick and effective planning, command and control, creating an EU Cyber-Command should be the first step. The Cyber-Command would be the hub-of-hubs for all cyber-related matters in the EU. It would be responsible for coordinating operational capacity in cyberspace by developing hard and offensive cyber-power concepts, in line with the logic of an *EU-centred* national security and superiority paradigm, in order to achieve the CSDP's operational goals under the Permanent Structured Cooperation framework. This Cyber-Command would follow the principles of trust among member states and EU institutions and agencies concerning the sharing of information and intelligence. In order to foster that trust, it should be led by both high-ranking military and civilian staff from each member state, on a rotating basis, and be responsible to the EU ministers of defence and the High Representative. The combination of military and civilian leadership would allow a better comprehension of cyber-threats and the reactions needed, taking into consideration the nature of the new 'battle-field' of cyberspace.

As pointed out by EDA Chief Executive Jorge Domecq, since its establishment the CSDP has been used to implement 30 military missions

[19] European Commission, 'Commission Signs Agreement with Industry on Cybersecurity and Steps up Efforts to Tackle Cyber-Threats', Press Release, 5 July 2016, accessed at http://europa.eu/rapid/press-release_IP-16-2321_en.htm on 17 July 2017.

[20] EPP, *EPP Paper on Security and Defence,* approved by the EPP Presidency and EPP Summit, 15 December 2016, accessed at http://www.epp.eu/papers/epp-paper-on-security-and-defence/ on 17 July 2017.

across the world;[21] yet since these have been carried out on an ad-hoc basis, without a command structure, there have been drawbacks to its functioning as well. This is another reason why an EU-level cyber-command is needed.

An example of a cyber-offensive capacity would be the use of cyber-capabilities to 'disrupt the communication of human traffickers in Libya to support the objectives of the EU naval operation Sophia off the Libyan coast'[22]; or the development of counter-narratives, addressing an external as well as an internal audience, which respond to the ever-increasing hybrid threats proliferating throughout cyberspace and social networks as a form of information warfare.[23]

To develop a cyber-offensive capacity coordinated by an EU cyber-command, the EU would need to revise its CFSP and CSDP instruments, aims and objectives. It would need to include a cyber-offence capacity in the operationalisation of the Mutual Defence Clause. The upcoming review of the EU Cyber Security Strategy will provide an opportunity to rethink the EU's cyber-strategy; to better define the roles and responsibilities between the EU institutions and agencies, member states, civil society, industry and academia; to connect the dots among stakeholders so that fragmentation is avoided; and to align the strategy within a common governance and command structure.

As a global actor, and through cyber-diplomacy, the EU should also seek consensus on rules, norms and enforcement measures in cyberspace, and also on international coordination in the detection of state-sponsored cyber-attacks and the use of international laws on persecution. The updated *Tallinn Manual* and Microsoft's proposal for a Digital Geneva Convention are worth exploring and debating.

[21] R. Singh, 'EDA Chief: EU Can No Longer Afford to Ignore Defence Policy', *The Parliament Magazine,* 29 March 2016, accessed at https://www.theparliamentmagazine.eu/articles/opinion/eda-chief-eu-can-no-longer-afford-ignore-defence-policy on 17 July 2017.

[22] M. Gahler, 'Towards a European Cyber Defence Policy', *The European Files* 40 (2016), 19, accessed at https://www.europeanfiles.eu/wp-content/uploads/2017/05/The-European-Files-Cybercrime-cybersecurity-cyberdefence-in-Europe-Issue-40-Janvier-2016.pdf on 17 July 2017.

[23] Ibid.

Conclusion and recommendations

There remains a lack of agreement regarding concepts related to cyberspace and cyberwar; yet despite this, many states are increasingly considering cyber-defence as an important capability and are allocating significant budget funds and personnel to developing not only cyber-defence, but also cyber-offence capabilities. The 2012 UN Institute for Disarmament Research assessment report found that 114 out of 193 member states of the UN had national cybersecurity programmes.[24] The report also suggested that 12 of the 15 largest military spenders have, or are developing, dedicated cyberwarfare units and that, of these, 10 appear to possess or to be developing offensive cyber-capabilities; of these, the US, the UK, China, Russia and France are generally seen as the most advanced in terms of power and capabilities. In short, numerous countries have strengthened their cybersecurity measures, *inter alia,* by building cyber-armies, developing cyber-weapons, conducting cyber-exercises and formulating ambitious cybersecurity policies.

It is clear that with the digitisation of our economies and societies in this interconnected world, more threats will appear that will have the potential to disrupt everyday life, as we have recently witnessed. When cyber-attacks devastate airport controls, banks, electricity grids or pipelines, they can constitute real acts of war that could lead to retaliation either in cyberspace or on the ground. It is thus of the utmost importance to look at how the EU should tackle this matter: whether, on the one hand, the EU maintains its current policies of developing cyber-defence and crisis management capacity or, on the other, the Union begins to use its entire capacity, at all levels, to create meaningful cyber-offence capabilities, like those that other 'nation blocs' are working on, in a coordinated and cooperative way. Concerning the latter alternative, below are some key policy recommendations:

- The EU should intensify the promotion of a single market for cybersecurity products (aligned with the Digital Single Market strategy) by fostering research, development and investment.

[24] UN Institute for Disarmament Research, *The Cyber Index: International Security Trends and Realities,* UNIDIR/2013/3 (2013), accessed at http://www.unidir.org/files/publications/pdfs/cyber-index-2013-en-463.pdf on 17 July 2017.

- Synergies should be created with projects such as the Galileo programme on satellite data for operations, and the European Open Science Cloud to develop a public–private—civilian–military cyber-ecosystem that generates the best innovation in the cyber-realm to tackle actual and upcoming challenges.

- A European university should be created that is able to attract and develop skilled workers beyond the traditional administrative and functional needs of the EU, teaching cyber-military skills in command and control, and also providing the technical training needed for specialists in data science, analysis, cyber-forensics, AI and robotics, within an overarching EU mindset.

- As much funding as possible should be derived from the myriad of EU funding programmes to develop the data infrastructure needed, the university and an ecosystem supportive of cyber-start-ups.

- An EU Cyber-Command should be established that is able to ensure quick and effective planning, command and control, and is also responsible for coordinating operational capacity in cyberspace by developing hard and offensive cyber-power concepts, in line with the logic of an EU-centred national security and superiority paradigm.

- The CFSP and CSDP instruments, aims and objectives should be revised to include cyber-offensive capacity in the operationalisation of Article 42(7) TEU.

- The EU Cyber Security Strategy should be revised to better define the roles and responsibilities between the EU institutions and agencies, member states, civil society, industry and academia within a common governance and command structure.

- The EU's cyber-diplomacy capacity and instruments should be strengthened across the board so that they can effectively reinforce the EU's norms and values, as well as lead action to reach consensus on the rules, norms and enforcement measures in cyberspace globally.

About the author

Gonçalo Carriço is the Digital Policy Officer at EPP Headquarters.

Credits

Wilfried Martens Centre for European Studies
Rue du Commerce 20
Brussels, BE - 1000

The Wilfried Martens Centre for European Studies is the political foundation and think tank of the European People's Party (EPP), dedicated to the promotion of Christian Democrat, conservative and like-minded political values.

For more information please visit: www.martenscentre.eu

Editor: Niklas Nováky, Research Officer, Martens Centre

External editing: Communicative English bvba

Typesetting: Victoria Agency

This publication receives funding from the European Parliament.

The European Parliament and the Wilfried Martens Centre for European Studies assume no responsibility for facts or opinions expressed in this publication or their subsequent use.

Sole responsibility lies with the author of this publication.