Strengthening the EU's Cyber Defence Capabilities

Report of a CEPS Task Force

Chair: Jaap de Hoop Scheffer

Rapporteurs: Lorenzo Pupillo
Melissa K. Griffith
Steven Blockmans
Andrea Renda

CEPS

Strengthening the EU's Cyber Defence Capabilities

Strengthening the EU's Cyber Defence Capabilities

Report of a CEPS Task Force

November 2018

Chair:	**Jaap de Hoop Scheffer**
Rapporteur and Coordinator:	**Lorenzo Pupillo**
Main Author:	**Melissa K. Griffith**
Co-Rapporteurs:	**Steven Blockmans**
	Andrea Renda

Centre for European Policy Studies (CEPS)
Brussels

CEPS is an independent think tank based in Brussels, whose mission is to produce sound analytic research leading to constructive solutions to the challenges facing Europe today. The views presented in this report do not necessarily represent the opinions of all participants in the Task Force, nor do they represent the view of any individual participant (unless explicitly mentioned in this report).

The views expressed in this report are those of the authors writing in a personal capacity and do not necessarily reflect those of CEPS or any other institution with which they are associated.

Cover illustration: Shutterstock/Titima Ongkantong

ISBN 978-94-6138-706-6

CEPS
Place du Congrès 1, B-1000 Brussels
Tel: 32 (0) 2 229.39.11
e-mail: info@ceps.eu
internet: www.ceps.eu

Table of Contents

LIST OF ABBREVIATIONS

AI	Artificial Intelligence
CCDOE	Cooperative Cyber Defence Centre of Excellence (NATO)
CERT	Computer Emergency Response Team
CERT-EU	Computer Emergency Response Team (for EU institutions)
CFSP	Common Foreign and Security Policy (EU)
CMF	Cyber Mission Force (CMF) teams (USCYBERCOM)
CNMF-HQ	Cyber National Mission Force Headquarters (USCYBERCOM)
CRM	Crisis Response Mechanism (for the EU's EEAS)
CSDP	Common Security and Defence Policy (EU)
CSIRT	Computer Security Incident Response Team
CSIRT Network	Computer Security Incident Response Team Network (EU)
DDoS attacks	Distributed Denial of Service attacks
DGs	Directorates-General (EU)
DG SANTE	Directorate-General for Health and Food Safety (EU)
EC3	European Cybercrime Centre (Interpol)
EDA	European Defence Agency (EU)
EEAS	European External Action Service (EU)
EGC	European Government CERTs group (EU)
ENISA	European Network and Information Security Agency (EU)
EU	European Union
EUMS INT	EU Military Staff Intelligence Directorate (EU)
FIRST	Forum of Incident Response and Security Teams
G-7	The Group of Seven
G-20	The Group of Twenty
GDPR	General Data Protection Regulation (EU)
GNSS	Global Navigation Satellite System
ICS	Industrial Control Systems
INTCEN	Intelligence Analysis Centre (in the EU's EEAS)
Interpol	International Criminal Police Organization

IoT	Internet of Things
IPCR	Integrated Political Crisis Response (EU)
ISAA report	Integrated Situational Awareness and Analysis report (EU)
IT	Information Technology
J-Cat	Joint Cybercrime Action Taskforce (Interpol)
MAD	Mutually Assured Destruction
NATO	North Atlantic Treaty Organization
NIS Directive	Network Information Systems (EU Directive on)
OESs	Operators of Essential Services (NIS Directive)
PESCO	Permanent Structured Cooperation (EU)
SITROOM	Situational Room (in the EU's INTCEN)
TF-CSIRT	Task Force on Computer Security Incident Response Teams
UK	United Kingdom of Great Britain and Northern Ireland
UN	United Nations
US	United States of America
USCYBERCOM	US Cyber Command
RPAS	Remotely Piloted Aircraft Systems

FOREWORD

The EU citizen has a right to a European Union that protects. Now, besides more 'classical' threats and challenges, cyberspace is being used to disrupt our daily lives. In the recent past, many cyberattacks emanating from nation states or individuals have caused substantial political, financial and economic damage. Both the public and private sectors are faced with the consequences, from election interference to attacks on critical infrastructure, from militarising cyberspace to the malicious exploitation of the Internet of things, where we see direct invasions of our privacy.

The moment has come for the European Union to strengthen its defences against present and potential disruptors and organise itself accordingly. This CEPS Taskforce has brought forward proposals to find a path from what has already been done to what could and should be done to streamline EU defences.

The members of the Task Force have grasped that a fine balance has to be found between the competences of the member states, primarily responsible for the wellbeing of their citizens, and those of the EU institutions, with their potential for creating the requisite added value of co-ordinating and streamlining procedures and initiating responses and potential actions. It is also imperative that the results of this exercise do not lead to 'turf wars' but instead greater integration between the EU actors involved.

Readers will note that we have strictly limited ourselves to the 'defensive' side of the discussion: how to best protect the EU citizen, public and private sectors against the consequences of aggressive cyber actions and attacks. To what extent member states and the EU are ready to become more proactive in the domain of reaction and possible retaliation was not within the remit of this Task Force.

We benefited from a very broad representation at the table, having been able to bring together all relevant actors, public and private alike. It is my hope that the resulting report will stimulate the debate on what can be achieved and how the European Union and its member states can best organise their defences against cyberattacks. And, equally important, I trust it may lead to a better and more efficient EU decision-making process to be able to act fast when necessary.

Jaap de Hoop Scheffer,
Chair of the Task Force
November 2018

PREFACE

This report is based on discussions in the CEPS Task Force on Strengthening the EU's Cyber Defence Capabilities. The Task Force, chaired by Jaap de Hoop Scheffer, Professor at Leiden University and Secretary General of NATO from 2004-2009, was composed of industry experts, representatives of EU institutions and agencies, of the technical community, of European governments, intergovernmental organisations and academics (see a list of participants in Annex 1). The group met on five separate occasions in the period between February 2018 and July 2018.

As Coordinator of the Task Force, I would like to acknowledge the invaluable contributions of all the participants in the Task Force to this work and also the contributions from our numerous invited guests. Particular thanks go to Melissa K. Griffith for her work in reporting the content of all the sessions and for her extensive writing of the report. I also wish to acknowledge the work done by my fellow rapporteurs, Steven Blockmans and Andrea Renda. Finally, I wish to thank Ada Modzelewska for her technical support.

Lorenzo Pupillo,
Rapporteur and
Coordinator of the Task Force
November 2018

EXECUTIVE SUMMARY

In an effort to strengthen EU cyber defence capabilities, this CEPS Task Force report puts forth:

I. a detailed analysis of key strategic and operational components of cyber defence,
II. the case for greater cyber defence coordination within the EU,
III. the development of three potential scenarios and the systematic evaluation of their relative strengths and limitations, and
IV. the final recommendation that the EU create a Cyber Defence Agency.

This report is the result of a collective effort led by CEPS, which launched on 22 February, 2018 at the CEPS Ideas Lab: a Task Force on Strengthening the EU's Cyber Defence Capabilities. The Task Force was composed of industry experts, representatives of EU and international organisations, academics, and practitioners (refer to Annex 1 for a full list of participants).

Meeting on five separate occasions between February and July 2018, the group explored:

- the characteristics of the cyber threat landscape;
- the challenges and dynamics of defence strategies, operation, and tactics; and previous and current defence approaches and
- best practices from EU Institutions, the European Defence Agency (EDA), the European Union Agency for Network and Information Security (ENISA), Israel, NATO, and the US.

These discussions led to the Task Force's recommendation, addressed to the EU's member states and institutions, for the development of a Cyber Defence Agency.[1]

A Cyber Defence Agency

The EU should not wait for a catastrophic event before acting to bolster EU cyber defence capabilities. Evidence collected by this CEPS Task Force confirms that the EU currently faces a clear and growing threat. This threat has triggered

[1] Note: not all participants support the recommendation of creating a cyber defence agency. As such, the views presented in this report do not necessarily represent the opinions of all participants in the Task Force.

mounting public awareness and rising demand for accountability, action, and fresh political will to tackle cyber defence concerns.

Trends in digital security threats, such as the proliferation of Internet of Things (IoT) devices and increases in reported vulnerabilities, have been accompanied by a series of profoundly worrying political and strategic trends.

1. States are actively militarising cyberspace.
2. States continue to represent the greatest potential for harm in cyberspace.
3. Offensive cyber capabilities are increasingly deployed within the context of two broader trends in conflict and warfare: hybrid operations and the use of surrogates.
4. Civilians are increasingly vulnerable victims of cyberattacks.
5. Efforts to apply norms to constrain state behaviour (in the context of war but also outside of war) have fallen short.

Yet, the EU's current cyber defence capacity is critically limited.

- The EU continues to play a largely advisory role, leaving the strategic and operational realities of cyber defence in the hands of member states.
- Existing capabilities are fragmented across, and siloed within, various institutions, agencies, and initiatives, which consequently undermines coordination and cooperation.
- Resources, both in terms of funding and personnel, are lacking.

In order to bolster the EU's capability to prevent and withstand cyberattacks, this CEPS Task Force identified a clear EU-wide interest for greater coordination and cooperation in this space. In view of the present lack of sufficient institutional capability and collaboration, and after a comparative analysis of alternative scenarios, the CEPS Task Force concluded in favour of creating an EU Cyber Defence Agency.[2]

Unlike the European Union Agency for Network and Information Security (ENISA), this agency would have executive competencies. Therefore, it would possess the ability to develop and utilise strategic and operational capabilities at the EU level. Notably, this executive function would not preclude a role for member states in cyber defence. Instead, a Cyber Defence Agency would share responsibility with EU member states to strengthen cyber defence analysis and capabilities within the Union.

[2] Note: not all participants support the recommendation of creating a cyber defence agency. As such, the views presented in this report do not necessarily represent the opinions of all participants in the Task Force.

The EU's executive responsibility would operate only when:

1. necessary corrective measures based on joint vulnerability assessment are not undertaken,
2. in the event of disproportionate cyberattacks, rendering the defence of a member state ineffective to such an extent that it risks putting in jeopardy the functioning of critical infrastructures elsewhere in the Union, or
3. when an incident targets EU institutions or programmes exclusively, such as the European Commission or Galileo.[3]

As a result, member states would have primary but not sole responsibility for the management of their cyber defence.

The Cyber Defence Agency should be built around 'core activities' that could be carried out with greater efficacy and/or efficiency through centralisation. These include coordination tasks such as the:

1. monitoring of EU policy implementation throughout disparate EU and member state agencies and institutions,
2. assessing the allocation of resources to institutions as necessary for the implementation of cyber defence strategies and operations,
3. facilitating communication and coordination across EU and member state agencies and institutions,
4. providing oversight of the entire EU defence architecture in order to maintain a cohesive EU readiness picture,
5. providing policy advice based on the observed readiness picture, and
6. serving as a single point of contact for EU institutions, member states and non-EU states.

The Agency would also develop core operational capabilities needed for preventing or withstanding a cyber incident occurring within the EU. These additional responsibilities – core activities – include, but are not limited to, the development of EU:

1. detection capabilities,
2. technical attribution capabilities, and
3. crisis response capabilities.

In the long term, stronger EU defence capabilities cannot be achieved through a largely segmented, multilevel governance model (the 2017 Cyber Security Package) or merely through the creation of a coordination mechanism (a cyber defence coordinator akin to the EU Counter-Terrorism Coordinator).

---

[3] Galileo is the EU's Global Satellite Navigation System (GNSS).

In contrast, the creation of an EU Cyber Defence Agency effectively addresses both the limitations of the current EU approach and ecosystem (fragmentation, a solely advisory role, and limited resources) as well strategic and operational considerations for developing a cyber defence posture more broadly. As such, it offers the greatest benefit towards achieving the goal of this Task Force: to strengthen EU cyber defence capabilities.

In recognition that – however preferable – an Agency cannot be created instantaneously, this CEPS Task Force has developed a series of stages leading to the final creation of a Cyber Defence Agency.

- Stage One
  - Implement the 2017 Cyber Security Package and the Cyber Defence Policy Framework.
- Stage Two
  - In coordination with ENISA, the Council and the Commission alongside other agencies such as the EDA, create a Cyber Defence Coordinator.
- Stage Three
  - Under the guidance of the Coordinator and through extensive collaboration with industry, implement a series of cooperation-oriented tasks that would lead to the development of a technical attribution forum.
- Stage Four
  - Under the guidance of the Coordinator, investigate and draft the mandate of and governance model for a Cyber Defence Agency.
- Stage Five
  - Create a Cyber Defence Agency that encompasses the coordinating functions of the Coordinator, ENISA's advisory capacity developed under the 2017 Package, and specific, core executive functions.

Given that cyberspace is increasingly used for strategic purposes, the EU cannot sit idly by. It risks a catastrophic policy failure unless it develops its own cyber defence capabilities to protect its citizens, institutions, and member states. In developing these capabilities, however, the EU must strike a balance between defending its civilians and avoiding the further militarisation of cyberspace.

Therefore, the EU should accompany its institutional efforts (creating the Cyber Defence Agency) with a commitment to implementing cyber norms through declaratory principles or an eventual guiding legal framework. These efforts have the potential to set standards for behaviour and conduct in cyberspace that simultaneously prevent attacks against the EU and extend protections to civilians outside the EU. These normative efforts are needed to encourage long-term and globally-embraced principles for peace in cyberspace.

1. INTRODUCTION

The European Union (EU) and its member states are a hub of economic activity and home to a large number of highly networked and interconnected countries. This makes cyberattacks a critical threat, and the resilience of each country a safeguard for the security of the whole EU.

The economic, social, and political costs of Europe's exposure to cyberattacks are real: 17 EU member states have been the target of election interference since 2004;[4] 900,000 Deutsche Telekom customers (Germany's largest telecom company) found themselves without service in 2016;[5] 9,000 people who collectively lost £2.5 million from their Tesco bank accounts during the same year;[6] one third of the UK's National Health Service was crippled in 2017, with thousands of appointments and operations cancelled;[7] Danish business conglomerate Maersk lost an estimated $200 - $300 million in the same year due to a single cyberattack;[8] almost half of UK businesses reportedly suffer a serious attack or breach over a 12-month period.[9]

---

[4] Oren Dorrell (2017), "Alleged Russian political meddling documented in 27 countries since 2004", *USA Today*, 7 Sept. (https://eu.usatoday.com/story/news/world/2017/09/07/alleged-russian-political-meddling-documented-27-countries-since-2004/619056001/).

[5] Auchard, Eric (2016), "Deutsche Telekom attack part of global campaign on routers", *Reuters*, 29 Nov. (https://www.reuters.com/article/us-deutsche-telekom-outages-idUSKBN13O0X4).

[6] Treanor, Jill (2016), "Tesco Bank cyber-thieves stole 2.5m pounds from 9,000 people", *The Guardian*, 8 Nov. (https://www.theguardian.com/business/2016/nov/08/tesco-bank-cyber-thieves-25m).

[7] Department of Health (2018), "Investigation: WannaCry cyber attack and the NHS", HC 414 SESSION 2017–2019, 25 April (https://www.nao.org.uk/wp-content/uploads/2017/10/Investigation-WannaCry-cyber-attack-and-the-NHS.pdf).

[8] Milne, Richard (2017), "Moller-Maersk puts cost of cyberattack at up to $300m", *Financial Times*, 16 August (https://www.ft.com/content/a44ede7c-825f-11e7-a4ce-15b2513cb3ff).

[9] "Cyber Security Breaches Survey 2018", UK Department of Digital, Culture, Media, and Sport (https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/702074/Cyber_Security_Breaches_Survey_2018_-_Main_Report.pdf).

Europe's already remarkable level of exposure will only increase, and rise steeply, in the coming years. Cyberspace, "a globalised network of networks",[10] underpins the daily functioning of critical infrastructure and vital services, governments and regional organisations, democratic institutions and public media, as well as militaries and businesses alike. For the EU, cyberspace has become an essential component of the Single Market as industry, innovation, and economic growth increasingly rely on information and communication technologies and activity becomes ever more networked.[11] The Digital Single Market strategy, one of the ten priorities set by Jean-Claude Juncker for his presidency of the European Commission, places the security and resilience of cyberspace in a constantly prominent role. Cyberattacks, as President Juncker argued in his 2017 State of the Union address, can be "more dangerous to the stability of democracies and economies than guns and tanks".[12]

However, cybersecurity is not only a question of secure infrastructure, effective defence, and emergency response. States around the world are actively militarising cyberspace through the development of offensive cyber capabilities and use of these tools to achieve geopolitical ambitions. Although estimates vary on the actual number of countries with significant offensive cyber capabilities, many experts confirm that the trend is on the rise: for example, former US Director of National Intelligence James Clapper warned in a 2017 congressional testimony that more than 30 countries were developing offensive cyberattack capabilities.[13] The enemy is often unknown, modes of attack are unpredictable, and the timing of attacks is equally uncertain. Attacks can take various forms, from state-sponsored offensives to commissioned Distributed Denial of Service (DDoS) attacks, manipulation of public opinion through "deep fakes" and other attacks on our democracies. With no global set of norms and no coordinated effort towards securing cyberspace, there is a real risk of a 'cyber Far West', an uncontrolled weaponisation of cyberspace, and the consequences are hard to imagine.

Evidence collected by the CEPS Task Force confirms that the EU currently faces a clear and growing threat, which is triggering mounting public awareness, a rising demand for accountability and action, and a growing political will to

---

[10] Singer, P.W. and Allan Friedman (2014), *Cybersecurity and Cyberwar: What Everyone Needs to Know*, (Oxford University Press; 1st edition).

[11] The Single Market seeks to ensure the free movement of goods, capital, services, and labour within the EU.

[12] Stupp, Catherine (2017), "Juncker announces massive cyber security overhaul" *EURACTIV*, 13 September, (https://www.euractiv.com/section/cybersecurity/news/juncker-announces-massive-cyber-security-overhaul/).

[13] https://www.armed-services.senate.gov/imo/media/doc/Clapper-Lettre-Rogers_01-05-16.pdf.

tackle cyber defence concerns. Hence, the time for the EU to act is now. But while the urge to act is widely acknowledged in the political debate, the type of actions to be undertaken, and the optimal allocation of responsibility and powers between the EU and the national level are much less clear, as the debate is often heavily affected by the lack of trust between member states, and the reluctance of national governments to give up sovereignty in favour of pan-European solutions.

Against this background, after collecting and elaborating available evidence on the threat landscape currently facing the EU, the CEPS Task Force identified a clear EU-wide interest for greater coordination and cooperation in this space. In view of the present lack of sufficient institutional capability and collaboration, and following a comparative analysis of alternative scenarios, it concluded in favour of creating an EU Cyber Defence Agency.[14] The main argument behind this proposal lies in the current fragmentation of EU's cyber defence capacity, which remains siloed within various institutions, agencies, and initiatives at different levels of government. Moreover, a crucial problem in the current EU landscape is that there is no standing model or an independent power for responding to cyberattacks. The creation of a fully-fledged agency would be an important step towards breaking down these silos and bringing all groups together to address the complex task of delivering on the promise of security and resilience for the Union in the cyber era. The creation of a new agency would also reflect a growing trend in EU multilevel governance, known as 'agencification', which aims at creating technocratic structures in which the EU and the national interest, together with private sector capabilities, can find a more effective synthesis. As observed in the academic literature, "agencies introduce more, and more flexible, administrative capacity and efficiency and facilitate, coordinate and strengthen cooperation between national authorities."[15]. We believe that these positive effects would also be felt in the field of cyber defence.

This report proceeds in five parts. Part I examines the evolving threat landscape facing the EU and its member states from both a technological and political perspective. It then complements these trends with a 'view from Europe'. Part II undertakes an evaluation of the range of potential defence

---

[14] Note: not all participants support the recommendation of creating a cyber defence agency. As such, the views presented in this report do not necessarily represent the opinions of all participants in the Task Force.

[15] Vos, Ellen (2018), "EU agencies on the move: challenges ahead", *Swedish Institute for European Policy Studies,* p. 17. For agencification in general, see Renda, A. (forthcoming), *Up, Down, and Sideways. The Endless Quest for EU's Optimal Multi-Level Governance*, forthcoming in Brousseau, E. (ed.) Oxford Handbook of International Economic Governance, Oxford University Press.

strategies and corresponding operational capabilities available to the EU. Part III conducts an analysis of the need for greater EU coordination in cyber defence. This includes a review of the current EU approach and its shortcomings. Part IV presents three potential scenarios for increasing EU cyber defence capabilities: (I) The Base Case: Implementing the 2017 Cyber Security Package, (II) Establishing a Cyber Defence Coordinator, and (III) Creating a Cyber Defence Agency. This section highlights how each scenario improves upon the existing institutional setup as well as outlining the remaining limitations of each. Part V advocates the creation of a Cyber Defence Agency, and explores in greater depth the added value of an agency in this domain. It also presents what could be a first step towards creating an agency ('II+'), which incorporates aspects of both Scenario II and Scenario III.

PART I
CYBER THREATS AND CYBER DEFENCE

2. THE EVOLVING THREAT LANDSCAPE

What threats are facing the EU and its member states? Which trends represent particular areas of concern? The threat space itself can be broken down into two broad categories: (i) technological trends in digital threats; and (ii) the militarisation and weaponisation of cyberspace. These two categories of activity highlight a rapidly evolving landscape both in terms of the scope and the severity of the threat. Ultimately, this rapidly evolving threat space has already affected and will continue to negatively affect the EU and its member states, through the economic impact, the frequency, and the broad scope of incidents.

2.1 Current trends in digital security threats

Digital security threats[16] range from the character of the terrain in need of defence and the proliferation of particular digital threats and attack vectors targeting this terrain. In the past few years, the attack surface has expanded exponentially along various dimensions, such as the terrain in need of defence, the proliferation of digital attacks, and notable changes in the attack vectors being used.

2.1.1 The terrain in need of defence is growing

In cyberspace, the terrain in need of defence is not a fixed or relatively limited space in contrast to the geographically bound terrains of air, land, and sea. Both the domain itself and the activity within it are entirely generated by human actions. With each new line of code and each new connected device, the terrain in need of defence expands. To a great extent, evolution and growth will remain inevitable characteristics of this terrain, but there are aspects to this growth and evolution that are not inevitable. For example, the pruning of excess code has not been a priority. As a result, the attack surface has become needlessly large. The relatively large attack surface found in cyberspace has important strategic implications for cyber defence that set it apart from other forms of defence,

[16] It is important to clarify here that while digital security threats and cybersecurity threats are often used interchangeably, this report is using the former to denote technological trends and the latter to encompass both technological and strategic trends in this space.

which face a relatively small and stable attack surface as their typical theatre of operations.

2.1.2 Reported vulnerabilities are rising steadily

The number of reported vulnerabilities is also growing.[17] In its 2018 Internet Security Threat Report,[18] Symantec reported that it witnessed a 13% increase relative to the previous year in overall reported vulnerabilities in 2017 and, even more concerning from a critical infrastructure perspective, a 29% increase in reports for industrial control systems (ICS).

The vulnerabilities of ICS and critical sectors should not be underestimated. While safety has historically been built into these systems, concerns over security (both digital and physical) have often been addressed only after the systems have been designed and built. In 2016 alone, we witnessed incidents in numerous critical sectors worldwide: communications (Deutsche Telecom[19] and Yahoo[20]), democratic institutions (the Democratic National Committee[21] and the Philippines Commission on Elections[22]), energy (the power grid in Ukraine[23]), financial services (the Central Bank of Bangladesh[24] and Tesco

---

[17] It is important to note, however, that increases in rates of observed and/or reported vulnerabilities should not be assumed to reflect actual or real increases in the number of vulnerabilities. Observed rates could increase while real rates remain constant, observed rates could increase while real rates decrease, or observed rates could increase at a slower rate than the increase in actual vulnerabilities. Observed vulnerabilities are just that: observed.

[18] "Internet Security Threat Report" Symantec. Volume 23 (https://img03.en25.com/Web/Symantec/%7Bf8ca1fb2-b73c-46d0-ae9e-17456c45df87%7D_ISTR23-FINAL.pdf?aid=elq_).

[19] Auchard, Eric (2016), "Deutsche Telekom attack part of global campaign on routers", *Reuters,* 29 Nov. (https://www.reuters.com/article/us-deutsche-telekom-outages-idUSKBN13O0X4).

[20] Goel, Vinu and Nicole Perlroth (2016), "Yahoo Says 2 Billion User Accounts Were Hacked", *New York Times*, 14 Dec. (https://www.nytimes.com/2016/12/14/technology/yahoo-hack.html).

[21] Lipton, Eric, David E. Sanger and Scott Shane (2016), "The Perfect Weapon: How Russian Cyberpower Invaded the U.S.", *New York Times,* 13 Dec. (https://www.nytimes.com/2016/12/13/us/politics/russia-hack-election-dnc.html).

[22] Chi, Leisha (2016), "Philippines elections hack 'leaks voter data'", *BBC* 11 April (https://www.bbc.com/news/technology-36013713).

[23] Greenberg, Andy (2017), "'Crash Override': The Malware that Took Down a Power Grid" *Wired,* 12 June (https://www.wired.com/story/crash-override-malware/).

[24] Gopalakrishnan, Raju and Manuel Mogato (2016), "Bangladesh Bank officials' computer was hacked to carry out $81 million heist: diplomat", *Reuters,* 18 May (https://www.reuters.com/article/us-cyber-heist-philippines/bangladesh-bank-officials-computer-was-hacked-to-carry-out-81-million-heist-diplomat-idUSKCN0YA0CH).

Bank[25]), healthcare (the Australian Red Cross[26] and National Health Service Hospitals in the UK[27]), IT services (domain name provider Dyn[28]) and security (the FBI and Homeland Security in the US[29]).[30]

While reported vulnerabilities have increased in general, the explosive growth of IoT (Internet of Things) devices simultaneously increases both the potential attack surface as well as introducing vulnerabilities. The IoT global market alone is expected to reach $8.9 trillion in 2020, compared to $2.99 trillion in 2014.[31] Not to mention that the expected number of connected devices globally, currently around one billion, is expected to reach one trillion by 2035 (according to ARM, a microprocessor supplier). This makes IoT a central area for concern and a significant contributing factor to the overall insecurity of the terrain.[32]

Finally, people remain perhaps the greatest and most enduring source of vulnerability. We introduce vulnerabilities both in terms of what we regularly

---

[25] Treanor, Jill (2016), "Tesco Bank cyber-thieves stole 2.5m pounds from 9,000 people", *The Guardian,* 8 Nov. (https://www.theguardian.com/business/2016/nov/08/tesco-bank-cyber-thieves-25m).

[26] ABC (2016), "Red Cross Blood Service admits to personal data breach affecting half a million donors", *ABC,* 28 Oct. (http://www.abc.net.au/news/2016-10-28/red-cross-blood-service-admits-to-data-breach/7974036).

[27] Erlanger, Steven, Dan Bilefsky and Sewell Chan (2017), "U.K. Health Service Ignored Warnings for Months", *New York Times,* 12 May (https://www.nytimes.com/2017/05/12/world/europe/nhs-cyberattack-warnings.html).

[28] Lewis, Dave (2017), "The DDoS Attack Against Dyn One Year Later", *Forbes,* Oct 23 (https://www.forbes.com/sites/davelewis/2017/10/23/the-ddos-attack-against-dyn-one-year-later/#2f68e96d1ae9).

[29] National Security (2016), "Justice, Homeland Security probe hack of U.S. agency employee data", *Reuters,* 8 Feb. (https://www.washingtonpost.com/world/national-security/dhs-and-fbi-investigate-possible-breach-of-employee-data/2016/02/08/98a09a9a-ceb8-11e5-abc9-ea152f0b9561_story.html?noredirect=on&utm_term=.bc55e51dd241).

[30] European Political Strategy Centre (2017), "Building an Effective European Cyber Shield: Taking EU Cooperation to the Next Level", *EPSC Strategic Notes*, Issue 24, 8 May, p. 2, (http://ec.europa.eu/epsc/sites/epsc/files/strategic_note_issue_24.pdf).

[31] Columbus, Louis (2017), "2017 Roundup of Internet of Things Forecasts", *Forbes,* 10 Dec. (https://www.forbes.com/sites/louiscolumbus/2017/12/10/2017-roundup-of-internet-of-things-forecasts/#6568c13e1480).

[32] CEPS has managed a Task Force on Software Vulnerability Disclosure in Europe from September 2017 to May 2018 and published a Report with a full set of recommendations. See https://www.ceps.eu/publications/software-vulnerability-disclosure-europe-technology-policies-and-legal-challenges.

do (open emails, click on links, visit webpages, plug in flash drives, etc.) and what we regularly fail to do (update systems, maintain backups, etc.).

2.1.3 Digital attacks proliferate

The scope of observed threats operating on this terrain and attempts to exploit vulnerabilities are likewise undergoing rapid evolution and proliferation. In 2017 alone, Symantec[33] reported a 92% increase in downloaded variants of malware, a 54% increase in variants of mobile malware, a 46% increase in ransomware variants and a 600% increase in IoT attacks compared to the rates observed in 2016 (see the graphic on the inside back cover).

2.1.4 Attack strategies and modes in constant evolution

The attack vectors utilised by hostile actors[34] on this terrain have evolved alongside trends in the growth of the attack surface, reported vulnerabilities and the payloads being deployed. According to Symantec's 2018 report, spearfishing[35] remains one of the most preferred attack vectors in 2017, recognising that humans remain one of the weakest links in the security of systems. In contrast to spearfishing, however, the observed use of zero-day vulnerabilities[36] is dropping off.[37]

Europol's "2017 Internet Organised Crime Threat Assessment" report highlights ransomware as a critical threat, examining how global ransomware campaigns have indiscriminately targeted both the public and private sectors alike, crossing borders, and affecting critical infrastructure. Europol also highlights 2017 as the first time serious botnet attacks utilised IoT devices, a trend which is only likely to continue.[38]

---

[33] "Internet Security Threat Report", Symantec, Volume 23 (https://img03.en25.com/Web/Symantec/%7Bf8ca1fb2-b73c-46d0-ae9e-17456c45df87%7D_ISTR23-FINAL.pdf?aid=elq_).

[34] Again, it is important to distinguish between observed attack vectors and actual attack vectors. Take the observed decrease in zero-days as an example. We may not observe them or locate them at previous rates, but that does not automatically mean they are not being used.

[35] A scam specifically tailored to individuals.

[36] A vulnerability in firmware, hardware, or software that is presently unknown to users but known by a potential attacker. Once used, the vulnerability becomes known and the system is patched or otherwise fixed, making it impossible to reuse the same vulnerability later in another attack against the same user or set of users.

[37] "Internet Security Threat Report", Symantec, Volume 23 (https://img03.en25.com/Web/Symantec/%7Bf8ca1fb2-b73c-46d0-ae9e-17456c45df87%7D_ISTR23-FINAL.pdf?aid=elq_).

[38] Europol (2017), "Internet Organized Crime Threat Assessment (IOCTA) 2017" (https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2017).

One particularly troubling development in attack vectors is the growing focus on compromising the software supply chain through software updates. While there were only four recorded software supply chain attacks in 2016, this rose on average, to one a month in 2017. This attack vector is particularly disturbing since it simultaneously represents both an efficient and rapid way to infiltrate big or large numbers of organisations given the widespread use of automatic updates within systems.

2.1. Trends in the weaponisation of cyberspace for strategic purposes

In addition to the technical evolution and characterisations of digital threats more broadly, one area of central concern is the weaponisation of this domain for strategic purposes by state and non-state actors. Cyberspace is not merely a technical domain. It is a political domain in which we are witnessing a growing use of cyber weapons for political ends. Given the range of politically motivated, state-sponsored attacks, 2016-17 notably represented an important inflection point for cybersecurity as a domain of strategic activity. We witnessed the widespread and indiscriminate targeting of civilians (WannaCry); targeting of civilian critical infrastructure (NotPetya); and the targeting of democratic processes through the acquisition and release of sensitive information from specific electoral campaigns (the 2017 French presidential elections), the general public and political elites through information operations leveraging social media (the 2016 US presidential elections), and the electoral infrastructure itself through results reporting platforms (the 2016 Ghanaian presidential elections).

These developments are particularly troubling for five reasons:

1. States are actively militarising cyberspace through the deployment of cyber tools for political ends, but also by pursuing these offensive cyber capabilities in the first place. Many governments now actively develop and stockpile offensive cyber weapons that can be used to target rival nations' militaries, infrastructure or citizens, as well as the property of private organisations. These weapons can seize control of data, shut down critical systems, and even destroy property, such as computers. The invisibility of these new weapons allows development to be obscured and often hard to recognise until the damage is already done in the form of an attack.
2. States continue to represent the greatest potential for harm in cyberspace. These targeted attacks – whether launched by states themselves, states utilising surrogates or proxies, or states deploying cyber means as part of a broader hybrid threat – represent the most dangerous form of activity in this threat space. Many have means that far exceed those of non-state actors and those means are deployed

towards a limited set of goals: espionage, disruption and/or financial gain. The victims of state and state-sponsored activity are always, ultimately, people and the economic costs can be extremely high. With an aggravating factor: attribution is often a daunting task.

3. Offensive cyber capabilities are increasingly deployed within the context of two broader trends in conflict and warfare: hybrid operations and the use of surrogates.[39] Both trends take advantage of traditionally held notions of inter-state conflict (e.g. the meeting of two militaries through the deployment of kinetic force as well as the boundary between peace and war) and alter the strategic dynamics of conflict (increased influence of individuals, low barriers to entry, deflection of responsibility, potential for escalation, etc.).
4. Civilians are substantial victims of cyberattacks. Over the past year, we witnessed the impact of cyber conflict on civilian populations following the WannaCry and NotPetya attacks. These attacks were not confined to military, intelligence, or other governmental targets. They were instead indiscriminate in nature, disabling and harming hospitals, schools, electric grids, and private companies. For example, the WannaCry attack impacted 200,000 computers running a Windows XP operating system in more than 150 countries, including many hospitals across the United Kingdom, responsible for providing life-saving care, that were suddenly unable to access critical systems and patient data, delaying treatments and sending emergency rooms into chaos. But even more concerning than the WannaCry attack itself was its origin. The ransomware exploited weaknesses that had allegedly been discovered and cultivated by the US National Security Agency before being stolen by hackers, and deployed by North Korea. The incident underscores just how quickly cyber weapons can be manipulated by malicious actors to devastating effect against unintended targets.
5. Efforts to apply norms (in the context of war but also outside of war) have fallen short. As a result of this militarisation and potential for escalatory conflict, governments have recognised the need to address cyber conflict and have done so through a number of multilateral and multi-stakeholder fora. In 2016, the Organization for Security and Co-operation in Europe adopted an enhanced list of "confidence-building measures (CBMs) to enhance security and stability in the cyber domain".

[39] Krieg Andreas and Jean-Marc Rickli (2019), Surrogate Warfare: The Transformation of War in the Twenty-first Century (Georgetown: Georgetown University Press, forthcoming.), and Krieg Andreas and Rickli Jean-Marc (2018), "Surrogate Warfare, The Art of War in the 21st Century?", *Journal of Defense Studies*, January, pp. 1-18 (http://www.tandfonline.com/doi/figure/10.1080/14702436.2018.1429218?scroll=top&needAccess=true#metrics-content).

In 2017, the Group of 7 (G7) published a declaration recognising the urgent need to establish international norms for responsible nation-state behaviour in cyberspace. To date, the primary mechanism has been the UN Group of Governmental Experts (UNGGE), which has focused on non-binding normative agreements of expected state behaviour. In June 2017, the group failed to come to an agreement on core aspects related to government behaviour, particularly around the applicability of international law in cyberspace. Notably, however, in a September 28, 2018 statement, US Deputy Secretary of State John J. Sullivan expressed American interest in restarting the norms dialogue through the UNGGE.[40]

The lack of progress in implementing agreed-upon cyber norms has enabled the continued militarisation of cyberspace. While many governments agree that international law exists and extends to behaviour in cyberspace, questions remain on how it applies in practice. This in turn has created a gap in the ability of international law to perform its humanitarian function, allowing nation-states to use offensive cyber means that put civilians at risk. The issue, therefore, is not a lack of potential legal or normative frameworks but rather in the lack of consistent implementation of existing frameworks. More work is needed to encourage principles for peace in cyberspace.

In conclusion, this threat landscape is simultaneously a technological and political domain. Moreover, over the past few years, we have witnessed equally important shifts in the technological and strategic aspects of this domain. Both sets of trends point to a rapidly evolving threat space in terms of the scope and the severity of the threat that the EU and its member states currently face.

2.2 The view from the EU

The EU is not immune to the effects – disruption and destruction – of this rapidly evolving threat space.

Being the largest single market in the world, the EU is a very attractive target for global cyberattacks. Europe is simultaneously responsible for a large share of global network transactions and serves as the origin for a large share of cyberattacks and malicious activity. According to risk firm ThreatMetrix's "2018 Cybercrime report: Europe Deepdive", Europe contributed 1.9 billion

[40] "On the Ministerial Meeting on Advancing Responsible State Behavior in Cyberspace" (https://www.state.gov/s/d/2018/286320.htm).

transactions out of the 9.3 billion global transactions they analysed in the first three months of 2018.[41] 58% of Europe's transactions utilised a mobile device, which is 7% higher than the global rate.[42] Europe is also a core hub for cyberattacks and malicious activities. In the same three-month period, Europe contributed to more than a quarter of all attacks, with 38% of all attacks originating from Europe. These rates are higher than for those originating in North America: ThreatMetrix reported 1.1 times the number of attacks from Europe as compared to North America over the three-month period.[43] As compared to the rates in the first three months of 2016, the growth in attacks outpaced growth in digital transactions by 86% in Europe.[44]

The EU and its member states have experienced a wide range of incidents where cyber weapons were deployed for political or strategic ends. According to the Alliance for Securing Democracy of the German Marshall Fund, 17 EU countries have been the target of election interference ranging from cyberattacks to disinformation campaigns: Bulgaria, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Hungary, Italy, Latvia, Lithuania, Poland, Portugal, Spain, Sweden, and the UK.[45]

The cost of cyber incidents extends far beyond democratic processes and institutions into social and economic costs effecting citizens and businesses alike. In 2007, outrage over Estonia moving a statue called the Bronze Soldier (originally called the "Monument to the Liberators of Tallinn", which celebrated the Russian victory of Nazism) from the city centre to a military cemetery led to protests, riots on the streets, and a series of cyberattacks targeting the online services of the government, media, and banks.[46]

---

41 ThreatMetrix (2018), "2018 Cybercrime report: Europe Deepdive: Insights from the ThreatMetrix® Digital Identity Network®", p. 4 (https://www.threatmetrix.com/digital-identity-insight/cybercrime-report/2018-cybercrime-europe/).

42 Ibid.

43 Ibid.

44 Ibid.

45 Oren Dorrell (2017), "Alleged Russian political meddling documented in 27 countries since 2004", *USA Today*, 7 Sept. (https://www.usatoday.com/story/news/world/2017/09/07/alleged-russian-political-meddling-documented-27-countries-since-2004/619056001/).

46 Damien McGuinness (2017), "How a cyber attack transformed Estonia", *BBC*, 27 April (https://www.bbc.com/news/39655415).

More recently, in 2017 the WannaCry ransomware attack, which crippled over one third of the UK's National Health Service (NHS),[47,48] while the NotPetya malware attack cost Maersk, the Danish business conglomerate, an estimated $200 -$300 million.[49,50] This year, in their 2018 "Cyber Security Breaches Survey" the UK reported that over the past 12 months almost half of all UK businesses suffered an attack or breach.[51]

These are not concerns of the past. Looking to the future, ENISA recently raised concerns over the development of 5G mobile networks, arguing that "fast mobile connections come with a 'medium to high risk' of cybersecurity attacks" and that "there are not enough safeguards in place to make sure the new networks will be secure".[52]

The costs for Europe are only likely to increase if attack trends persist. In 2017, a Lloyd's of London report estimated that the economic losses from a global cyber-attack would be comparable to those incurred from Hurricane Katrina in 2005.[53] In two scenarios they examined – an attack causing a widely-used cloud-service provider to fail and an attack that exploited a vulnerability in a widely-used software – they estimated costs of up to $53 billion and $28.7

---

[47] Department of Health (2018), "Investigation: WannaCry cyber attack and the NHS", HC 414 SESSION 2017–2019, 25 April (https://www.nao.org.uk/wp-content/uploads/2017/10/Investigation-WannaCry-cyber-attack-and-the-NHS.pdf).

[48] The attack was attributed to North Korea by companies such as Microsoft and states such as the UK. Phil Muncaster. 2017. "UK Government Blames WannaCry on North Korea". *Info Security*. 30 Oct. (https://www.infosecurity-magazine.com/news/uk-government-blames-wannacry-on/).

[49] Milne, Richard. 2017. "Moller-Maersk puts cost of cyberattack at up to $300m" *Financial Times*. 16 August (https://www.ft.com/content/a44ede7c-825f-11e7-a4ce-15b2513cb3ff).

[50] The attack was attributed to Russia by private sector firms and states such as the US and UK. Sarah Marsh (2018), "US joins UK in blaming Russia for NotPetya cyber-attack", *The Guardian*, 15 Feb. (https://www.theguardian.com/technology/2018/feb/15/uk-blames-russia-notpetya-cyber-attack-ukraine).

[51] "Cyber Security Breaches Survey 2018". UK Department of Digital, Culture, Media, and Sport (https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/702074/Cyber_Security_Breaches_Survey_2018_-_Main_Report.pdf)

[52] Stupp, Catherine. 2018. "Cybersecurity agency warns of 'extremely dangerous' risks of 5G technology" *EURACTIV*. 29 March (https://www.euractiv.com/section/cybersecurity/news/cybersecurity-agency-warns-of-extremely-dangerous-risks-of-5g-technology/).

[53] Ricadela, Richard. .*2017*. "Europe's Cyber Victims Are Racking Up Hundreds of Millions in Costs" *Bloomberg*. 3 August (https://www.bloomberg.com/news/articles/2017-08-03/europe-s-cyber-victims-racking-up-hundreds-of-millions-in-costs).

billion respectively.[54] In a survey of 127 European IT and security professionals, Black Hat concluded that "77% of respondents believe a cyberattack will breach critical infrastructure across European countries within the next two years" and "42% say cyber espionage by major nation-states such as Russia and China and attacks by rogue nations such as North Korea pose the biggest threat to EU critical infrastructure".[55]

In conclusion, for the EU and its member states, the economic, political, and social costs of cyberattacks are not hypothetical. They are increasingly a costly reality for states, industry, and the citizenry alike.

[54]Suess, Oliver (2017), "Global Cyber Attack Could Cost $121.4 Billion, Lloyd's Estimates", *Bloomberg*, 18 July (https://www.bloomberg.com/news/articles/2017-07-18/global-cyber-attack-could-cost-121-4-billion-lloyd-s-estimates).

[55] Black Hat (2017), "2017 Black Hat Europe Survey: The Cyberthreat in Europe", p. 4 (https://www.blackhat.com/docs/eu-17/Black-Hat-Attendee-Survey.pdf).

3. KEY COMPONENTS OF CYBER DEFENCE

Given the threats facing the EU's member states and its own institutions, how can the EU and its member states bolster their ability to detect vulnerabilities and incidents, mount an active defence in real-time as an incident is unfolding, and deter potential adversaries from carrying out attacks in the future?

An important focus of this Task Force has been to examine how the EU can defend their populations from cyberattacks. What does cyber defence entail? What are the range of potential strategies that an actor may pursue and what capabilities are needed to successfully implement those strategies?

This section of the report discusses two core pillars of a defence posture – preventing and withstanding an attack – and examines potential strategies for achieving these goals as well as potential limitations of each strategy within the specific context of cyber defence. It concludes with an overview of three core capabilities – detection, attribution, and incident response – needed for pursuing these pillars/goals.

3.1 Defining the scope

Cyber defence, like cyber security, is a term that covers a wide range of activity. For this Task Force, cyber defence is understood as a core component of the security of society:[56] defending the core functioning of the EU and its member states. As such, it is broadly defined to include the defence of people, industry, institutions, and governments within the EU. As well as EU and member state civilian and defence institutions, this incorporates democratic processes, such as elections (from voter rolls to ballot casting, ballot tallying to the certification of results, and from campaign advertisements to financial contributions). Cyber defence also includes the EU Single Market, including the Digital Single Market, and private industry and organisations within and across member states. In other words, cyber defence is the strategic and operational task of protecting

[56] Finland's 2013 Cyber Security Strategy uses this term to describe a broader security goal, of which cyber security is merely one component (https://www.defmin.fi/files/2378/Finland_s_Cyber_Security_Strategy.pdf).

populations, to the best of one's ability, from significant harm due to cyber actions (attacks, incidents, campaigns, or operations) of an external power.

This understanding of cyber defence as a component of a broader defence of society is not new, either within some European states' historic understanding of national security or within many states' focus on critical services or sectors in their own cyber security strategies.

For example, historically, Finland has understood that national security "is directly tied to the interdependencies between different actors [both public and private] as well as the management and harmonisation of these various actor's goals and interests".[57] Cyber security is no different, requiring specific action by government agencies and private industry alike. In other words, defence of society requires a cyber defence strategy recognising that in order to "safeguard its independence and territorial integrity", both "public and private actors alike can be and often are security actors (*turvallisuustoimija*), critical in maintaining and providing for the vital functions of society (*yhteiskunnan elintärkeä toiminto*) in times of crisis".[58]

In a more broad sense of cyber security policies, the recognition that cyber defence encompasses the defence of both the public and private sectors of society can be found in the heavy focus on protecting the vital functioning of society, often referred to as essential services and infrastructure or critical sectors. Significantly, efforts in Germany, France, the Netherlands, and the UK to view electoral systems as "as part of critical infrastructure" and their approaches to "institutionalise preparations to protect election processes, and broaden activities to the subnational levels" have been highlighted by those seeking to better understand this component of defence of society and in an effort to bolster US cyber defence as one component of electoral security.[59]

---

[57] Griffith, Melissa K. (2018), "A Comprehensive Cyber Security Approach: Bolstering Cybersecurity Capacity through Industrial Policy", *BASC Working Paper Series*, BWP18-07, p. 7 (https://basc.berkeley.edu/wp-content/uploads/2018/09/BWP18-07.pdf).
Note: This paper is part of a project "Comparative Industrial Policy in the Cyber Security Industry: Policies, Drivers, and International Implications", organised by Vinod K. Aggarwal and Andrew Reddie of the Berkeley APEC Study Center and funded by the Center for Long-Term Cybersecurity at the University of California, Berkeley. Other country cases include countries such as Japan, the UK, and the US.

[58] Ibid.

[59] Brattberg, Erik and Tim Maurer (2018), "Russian Election Interference: Europe's Counter to Fake News and Cyber Attacks", *Carnegie Endowment for International Peace*, 23 May (https://carnegieendowment.org/2018/05/23/russian-election-interference-europe-s-counter-to-fake-news-and-cyber-attacks-pub-76435).

Moreover, the EU itself has further mirrored this "security of society" approach to cyber security in its NIS Directive, which is discussed in greater detail later in this report but which calls for greater "national supervision of critical sectors":

> EU Member states have to supervise the cybersecurity of critical market operators in their country: Ex-ante supervision in critical sectors (energy, transport, water, health, and finance sector), ex-post supervision for critical digital service providers (internet exchange points, domain name systems, etc.).[60]

Current and past strategies and the operational requirements of emerging strategies draw further attention to the reality that cyber defence is best understood as a defence of society issue, which includes not only military operations and defence forces but also national and regional economies, civil society, and fundamental civilian wellbeing.

It is worth noting that responsibility for cyber defence, given this broad, societal definition, is often broken down nationally and internationally between civilian and military and public and private actors. While significant focus so far has been paid to the civilian components of cyber defence – e.g. the security and resilience of critical infrastructure and services such as energy, there is also a national or regional defence component in the military context and that of kinetic warfare.

Therefore, a component of the broader societal defence can be achieved through military operations. As such, cyber defence emphasises questions of how to integrate cyber capabilities into military organisations and operations most effectively, how to maintain cyber superiority on the battlefield as part of an ongoing engagement, and how to develop and deploy cyber capabilities. In this context, many member states have established Cyber Commands and recognised cyberspace as a domain of warfare alongside air, land, sea, and space.[61] Cyberspace represents both a domain of operations in and of itself and a vital component of military operations. Modern weapon and sensor systems – be they air, land, sea, or space – are packed with embedded digital systems. Connectivity is key to their success, while simultaneously representing a critical vulnerability.

In terms of military organisation and operations, armed forces within the EU must also consider how best to design future systems to address concerns

---

[60] EU NIS Directive (https://www.enisa.europa.eu/topics/critical-information-infrastructures-and-services/cii/nis-directive).

[61] Smeats, Max and Herbert S. Lin (2018), "Offensive Cyber Capabilities: To What Ends?", Cycon X Conference Proceedings (https://ccdcoe.org/sites/default/files/multimedia/pdf/Art%2003%20Offensive%20Cyber%20Capabilities.%20To%20What%20Ends.pdf).

such as military cloud computing environments, advanced and protected communications and data systems, self-defending and autonomous systems, all defining a new generation of military capabilities. For example, we are currently experiencing rapid development in Remotely Piloted Aircraft Systems (RPAS) towards becoming more autonomous systems that will find their place on the battlefields of the future. This introduces new cyber security challenges, not only in wartime but also for peacetime Common Security and Defence Policy (CSDP) missions. Increased automation and autonomy represent a paradigm shift from "Human-in-the-loop" to "Human-on-the-loop" scenarios in which it will be necessary that systems have the capability to make decisions themselves with consideration of their situational awareness and mission goals. To create such systems with the highest degree of reliability, security and resilience, cyber security becomes paramount from the earliest stage of research to development of the technology. The challenge of creating this generation of capabilities and updating existing ones to reach the same level of maturity is extremely complex and obliges each individual EU country to address a list of priorities with few resources to cover them all: in this context, international cooperation for capability development, supported by a coherent and coordinated approach, is the only recipe for success.

Another example is data protection, as data are clearly an essential asset in all missions. The EU and its member states will have to ensure data confidentiality, integrity and availability in an interconnected scenario such as will be introduced with System Wide Information Management (SWIM). This concept foresees that all aviation stakeholders, including military aviation, will be part of one global information exchange infrastructure that relies on the use of Commercial Off-The-Shelf (COTS) systems. It will improve coordination between civil and military aviation, but also introduces cyber security challenges. Besides ensuring safety and security for pilots and passengers, the EU and its member states will also need to safeguard essential data from cyber threats.

These areas present specific questions which are not the sole or even primary focus of this Task Force, which focuses more on the civilian side of cyber defence. However, given the role of organisations such as the EDA in EU member state defence force cooperation and coordination, they are quite relevant to EU efforts in this space and call for efforts to ensure coordination and coherence between all players.

3.2 Strategies in cyber defence

This Task Force has identified two central goals of any defence posture: preventing an attack from occurring in the first place and then subsequently

withstanding an attack if prevention fails. Under each of these goals, there are a range of potential strategies an actor can pursue.

It is important to note that efforts to prevent and withstand an attack do not occur in isolation but rather as complementary components within an overarching defence posture. Moreover, some of the capabilities developed or efforts undertaken to prevent an attack may also prove useful later when working to withstand an attack. As such, the pursuit of one goal does and should not preclude the pursuit of the other.

3.2.1 Preventing an attack: classical deterrence and dissuasion

Prevention is a fundamental pillar in any cyber defence posture. The objective is to avoid an altercation from occurring in the first place. There are two dominant and interrelated approaches to prevention: (i) deterring an adversary and (ii) dissuading an adversary. Both deterrence and dissuasion strategies seek to raise the cost of an attack relative to the potential benefits gained from such an attack, and in so doing alter the preferences of the potential aggressor.[62]

Deterring an aggressor

In its most general formulation, deterrence[63] is a strategy seeking to alter an adversary's behaviour by discouraging a specific aggressive action against a specific set of states or targets. Put another way, "whether broadly or narrowly defined, deterrence dissuades people or diminishes the likelihood of bad behavior by making them believe that the costs of their actions to them will exceed the benefits".[64]

Although deterrence is often deployed as a standalone term in discussions, there are in fact a range of mechanisms through which an actor can

---

[62] Joseph Nye in his 2017 *International Security* article titled, "Deterrence and Dissuasion in Cyberspace" covers four mechanisms for deterring and/or dissuading an adversary: deterrence by punishment, deterrence by denial, deterrence by entanglement, and deterrence by norms/taboos. The first two of these mechanisms – punishment and denial – comprise what is commonly referred to as classical deterrence, while the latter two – entanglement and norms/taboos – had previously been placed into broader discussions of dissuasion and of altering the strategic behaviour of states. As such, these four mechanisms are discussed in this report but separated into classical deterrence versus broader dissuasion categories.

[63] For a detailed breakdown of the existing research on deterring cyberattacks, refer to Melissa K. Griffith and Adam Segal's 2018 White Paper, entitled "International Security and the Strategic Dynamics of Cybersecurity" prepared for the Cyber Conflict Studies Association (CCSA)'s annual Cyber Conflict State of the Field meetings, which serves as an overview of the types of questions being asked and the research that has been conducted in international security related to cyber conflict. One sub-section focuses on debates and consensus around deterrence in the context of cyber conflict.

[64] Nye, Joseph S. (2017), "Deterrence and Dissuasion in Cyberspace", *International Security* 41(3): p. 53.

deter potential adversaries. Since the advent of nuclear weapons, for example, and the subsequent nuclear deterrence strategy of Mutually Assured Destruction (MAD), deterrence has often been assumed to be synonymous with punishment or retaliation in kind. However, deterrence is more than just this. Indeed, classical deterrence strategies have focused on (i) raising the relative cost of an attack through punishment (deterrence by punishment) and/or (ii) denying benefit from an attack (deterrence by denial).

Punishment relies on a particular and credible threat of retaliation in response to a specific hostile action undertaken by a specific adversary. Unlike MAD, however, not all punishment must be in kind. For example, punishment can be imposed within the same domain (e.g. a cyberattack precipitating another cyberattack in response), across domains (e.g. a cyberattack leading to a kinetic response), or entirely non-military in character (e.g. imposing sanctions in response to a cyberattack). Punishment can be threatened but not yet carried out (e.g. the threat of nuclear retaliation deterring a nuclear attack) or previously carried out (e.g. sanctions imposed in response to a previous incident deterring a similar incident in the future).

In the context of cyber defence, there are clear limitations to classical punishment models of deterrence. Namely, there are certain capabilities that are essential for punishing or signalling the intent to punish. The most commonly discussed of these capabilities is attribution. One cannot punish an unknown or ambiguous attacker. In cyberspace, hostile actors have an easier time hiding behind plausible deniability than in air, land, and sea. In order to retaliate, it is critical to know against whom you are retaliating. Hence, there is an attribution problem in cyber defence[65] that inhibits the utility of preventing an attack through the threat of retaliation. While attribution is not the only concern[66] in

[65] For examples of work focusing on the attribution problem see Clark, D. and D., Landau (2011), "Untangling Attribution", *Harvard National Security Journal* 2(2); Lindsay, Jon R. (2015), "Tipping the scales: the attribution problem and the feasibility of deterrence against cyberattack", *Journal of Cybersecurity* 1(1): 53-67; Rid, Thomas and Ben Buchanan (2015), "Attributing Cyber Attacks", *Journal of Strategic Studies* 38(1–2) (January): 4–37; and Healey, Jason (2016), "Beyond Attribution: Seeking National Responsibility in Cyberspace", *Atlantic Council*.

[66] To name a few, concerns around (i) asymmetric vulnerability as well as the ability to (ii) signal and (iii) tailor effects have also been raised within the context of single domain retaliation. For example, all states are vulnerable to a nuclear attack but not all states are similarly vulnerable to a cyberattack. Vulnerability is a function of both digital dependence and the potential attack surface. Some countries are far more digitally dependent and have far greater attack surfaces than others. This asymmetry makes retaliation difficult if the adversary is far less vulnerable to the types of tools they have deployed against others. In addition, signalling a credible capacity to retaliate is a particular challenge if an actor wishes

'prevention through punishment' approaches to cyber defence, it is by far the most fundamental as the inability to assign responsibility undermines the ability to punish, in any form.

Denial, in contrast, seeks to repel or undermine the overall success of any given attack/incident. The hope of a denial-based deterrence strategy is that as the potential benefits decrease, adversaries will be less willing to implement hostile actions. Like punishment models, denial models rely not only on the ability to repel an ongoing attack but also to make that ability known to potential adversaries in advance of any attack. If an adversary is not aware that denial is possible, it cannot be part of their decision-making process when deciding whether or not to attack. In short, deterrence by denial strategies seeks to harden potential targets and in so doing, dissuade potential adversaries from targeting them in the first place.

Denial-based deterrence is also not without its limitations in the context of cyberspace. Namely, denial can never be 100%. While hardening some targets may deter some forms of cyber incidents, it is unlikely to deter actors that have strong strategic interests at stake and are therefore willing to pursue their goals at a higher cost to themselves. Moreover, although deterrence by denial has become a buzzword deployed whenever bolstering cybersecurity and resilience is mentioned, it is hard to assess whether denial-based strategies have altered any given actors' willingness to carryout cyberattacks in practice.[67]

---

to retaliate in kind as signalling capability to retaliate using cyber tools can be challenging. Offensive cyber capabilities are less visible than their kinetic counterparts and often have far more limited life-spans. Finally, given the unpredictability of the effect and spread of many types of cyberattacks, it is more difficult to tailor a proportional response or limit collateral damage with cyber tools than with kinetic tools. These issues are not insurmountable, however. For example, Gartzke, Erik and Jon R. Lindsay (2015), "Weaving Tangled Webs: Offense, Defense, and Deception in Cyberspace", *Security Studies* 24(2) (April): 316–48, focus on alternatives to punishment-in-kind for overcoming concerns around signalling and asymmetries in vulnerabilities.

[67] There are two additional concerns around denial-based deterrence strategies of note. First, given the pace at which cyberspace and the suite of related technologies is evolving, maintaining highly secure and resilient systems requires significant resources and constant attention. The costs it imposes on potential targets, independent of what it imposes on potential adversaries, is quite high. Second, if cyberspace favours the offense, then deterrence through denial will prove to be far costlier to states than the offensive operations targeting those states. Put another way, all else being equal, it is costlier to defend one's own use of cyberspace through resilience and security than it is to disrupt an adversary's use of cyberspace.

Note that there is widespread support in academic and policy circles for viewing cyberspace as offense dominant. However, a vocal minority are simultaneously pushing back against the

Dissuading an aggressor

Beyond the classical deterrence strategies, the broader (or perhaps, parent category) of dissuasion offers two additional models for preventing an incident from occurring. Harvard University's Joseph Nye in his 2017 article draws policymakers' attention to two specific dissuasion strategies (i) norms/taboos and (ii) entanglement.[68] While both are useful in theory, in practice they have so far proven to be limited.

Unlike classical deterrence strategies, **norms/taboos** attackers are dissuaded by the prospect of the international community imposing reputational costs on anyone who violates specific codes of conduct in cyberspace.[69] Norms are not without success. They have altered state behaviour before: norms against the use of landmines and chemical weapons are two classical examples.

However, it is challenging to establish norms and their success in cyberspace, in particular, remains limited. Normative efforts are already underway, but they currently fall below the threshold of an established norm. For example, the US, through the United Nations (UN), spearheaded an effort to develop a norm against targeting essential services and infrastructure.[70]

---

claim that offense has the upper hand. For examples of the former, refer to Libicki, Martin C. (2007), *Conquest in Cyberspace: National Security and Information Warfare* (New York: Cambridge University Press); Nye, Joseph S. (2010), "Cyber Power", Essay from the *Belfer Center for Science and International Affairs*, Harvard Kennedy School (May); Liff, Adam P. (2012), "Cyberwar: A New 'Absolute Weapon'? The Proliferation of Cyberwarfare Capabilities and Interstate War", *Journal of Strategic Studies* 35(3): 401-428; Kello, Lucas (2013), "The Meaning of the Cyber Revolution: Perils to Theory and Statecraft", International Security 38(2): 7–40; and Lieber, Keir (2013), "The Offense-Defense Balance and Cyber Warfare", in Emily O. Goldman and John Arquilla, eds., *Cyber Analogies* (Monterey, Calif.: Naval Postgraduate School). For examples of the latter refer to Lindsay, Jon R. (2013), "Stuxnet and the Limits of Cyber Warfare", *Security Studies* 22(3): 365-404; Rid, Thomas (2013), *Cyber War Will Not Take Place* (Oxford: Oxford University Press). For a more comprehensive review of the literature on offense-defence dominance in cyberspace refer to Melissa K. Griffith and Adam Segal's 2018 White Paper, entitled "International Security and the Strategic Dynamics of Cybersecurity" prepared for the Cyber Conflict Studies Association (CCSA)'s annual Cyber Conflict State of the Field meetings.

[68] Nye, Joseph S. 2017. "Deterrence and Dissuasion in Cyberspace", *International Security* 41(3).

[69] Ibid. p. 60.

[70] UN Secretary-General (2015), "Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security", United Nations General Assembly, 22 July (http://www.un.org/ga/search/view_doc.asp?symbol=A/70/174).

However, this process ended in deadlock in 2017.[71] Even private companies have begun to undertake normative efforts in this space. Microsoft, for example, has championed the need for the principles for peace building measures in cyberspace (one notable example is the French government's call for trust and security in cyberspace) to protect civilians from cyberattacks in times of peace.[72] On the legal front, the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) has made significant progress analysing the applicability of existing international law to the cyber domain.[73] Yet, even here it remains uncertain if states will abide by these interpretations and, moreover, if they will function as norms with significant censure emerging when and if they are violated. Additionally, much of international law hinges on punishment-based rather than normative mechanisms in its implementation. Ultimately, as a preventive strategy, norms-based dissuasion strategies have a mixed track record and remain a strategy requiring long time horizons before potential benefits could be grasped.

One final strategy for preventing cyberattacks is **entanglement.** Unlike norms, which seek to dissuade adversaries from carrying out specific types of cyberattacks, entanglement dissuades hostile action in general between specific sets of actors due to significant interdependencies. One popular articulation of the potential to increase the costs of an attack through interdependency stems from 19th century liberal economics, which argued that commerce between states provides security externalities by making armed conflict costlier to all parties involved. The logic of entanglement was further developed in the 20th century with the introduction of Complex Interdependence, which broadened the scope of interdependencies beyond commerce and argued that given the complex web interdependencies between states, successful attacks against one state would simultaneously impose serious costs on both the aggressor and the victim.[74]

---

[71] Segal, Adam (2017), "The Development of Cyber Norms at the United Nations Ends in Deadlock. Now What?", The Council on Foreign Relation's *Net Politics* and *Digital and Cyberspace Policy Program*, 29 June (https://www.cfr.org/blog/development-cyber-norms-united-nations-ends-deadlock-now-what).

[72] French Ministry of Foreign Affairs (2018), "Cybersécurité : Appel de Paris du 12 novembre 2018 pour la confiance et la sécurité dans le cyberspace", Paris Peace Forum, 12 November (https://www.diplomatie.gouv.fr/fr/politique-etrangere-de-la-france/diplomatie-numerique/la-france-et-la-cybersecurite/article/cybersecurite-appel-de-paris-du-12-novembre-2018-pour-la-confiance-et-la).

[73] The Tallinn Manual 2.0 can be accessed from the NATO CCDCOE website: https://ccdcoe.org/research.html.

[74] Keohane, Robert O. and Joseph S. Nye Jr. (2011), *Power & Interdependence (4th Edition)*, Longman Classics in Political Science, Pearson.

Unlike punishment, denial, and norms, entanglement is an indirect preventive strategy. It is worth noting that cyberspace itself has led to a significant increase in the entanglement between states. By its very definition, cyberspace is a globalised network of networks. On the one hand, this brings with it a very real risk of contagion effects across networked systems independent of national boundaries. On the other hand, the more reliant a state becomes on cyberspace, the greater the cost of destabilising this foundational component of economy, society, and national defence potentially becomes for the state concerned. Yet, while we currently live in a highly interconnected world with significant entanglements between potential rivals, we still observe cyberattacks, a growing threat space, and the weaponisation of cyberspace. Similar to normative approaches to dissuasion, entanglement operates better in theory than in practice. Overall, there can be no single actor governing or controlling the entire space; this makes it an ideal candidate for coordinated efforts between EU member states.

3.2.2 Withstanding an attack: security and resilience

If and when prevention fails, defence rests upon the ability of an actor to withstand or repel an ongoing attack. This strategy, sometimes referred to as cyber preparedness, focuses on the processes and technologies that are used to safeguard critical assets. Withstanding an incident has two dynamics of note: (i) increasing security and (ii) increasing resilience.

Security

Increasing security entails measures taken to address vulnerabilities and potential attack vectors (e.g. firewalls, virus and malware detection software, and software patches and updates). This occurs through a focus on the people using the systems, the processes deployed to secure those systems, and the technology both in terms of involving vulnerabilities and also of providing assets for potential security solutions for those systems. For example, nuclear weapons are often protected by a series of security measures, such as limited access to physical sites. In cyberspace, as with nuclear weapons, increasing the level of security can force potential adversaries targeting certain systems to expend far more resources in order to achieve their goal.

Resilience

Increasing resilience, in contrast, focuses on maintaining the core functions of the broader system if an attack or incident takes place. Put another way, resilience is the ability to carry out core functions in the event of a successful attack rather than the ability to avoid an incident all together. Returning to the nuclear analogy, nuclear defence architecture often has specific aspects of resilience built in if security fails. For example, nuclear missile silos, ballistic

missile submarines, and nuclear bombers all serve as a failsafe for each other in the event that one or more are compromised. Increasing resilience in cyber defence decreases the degree and scope of damage an incident can generate through mechanisms such as data backups, parallel systems, and limiting single points of failure.

A commonly accepted definition of cyber resilience includes four core tasks: anticipate, withstand, recover, and evolve. Resilience, therefore, requires solid threat intelligence to pre-empt attacks or incidents, detection capabilities and incident response once an attack is ongoing that allow for efficient recovery, and a focus on lessons identified/learned and/or research and development in order to increase resilience over time.

Significantly, "Building Resilience and taking an Integrated Approach to conflicts and crises" are two strategic priorities identified in the 2016 EU Global Strategy.[75]

In the nuclear architecture example, security and resilience measures do not occur in isolation of each other. They combine together to create a high level of preparedness/ability to withstand a potential attack. Likewise, in an era of cyber conflict, defending the EU and its member states' use of cyberspace requires a pantheon of security and resilience measures. These measures, however, have a much broader scope to grapple with given that cyberspace underpins the 21st century. Defence in this space requires a focus on the vital functions of society (critical infrastructure and essential services). Uniquely, given the significant breadth of cyberspace, cyber resilience and security measures for the purpose of defence will also be useful in addressing other areas of concern, such as cybercrime or failures/cascades stemming from accidents or natural disasters.

3.3 Key operational capabilities

Both prevention-based and preparedness-based strategies for cyber defence face unique operational challenges, such as detection, attribution, and incident response capabilities. These are by no means meant to represent the entire universe of necessary tactical and operational capabilities but rather provide a foundation for and sampling of the critical operational dynamics of cyber defence. There are operational capabilities, threat intelligence capabilities for example, that are not present in this section but remain critical components to both prevention-based and preparedness-based strategies.

---

[75] The EU Global Strategy (2016), "From Vision to Action - Strategic Priorities of the EU Global Strategy" (https://europa.eu/globalstrategy/en/global-strategy-foreign-and-security-policy-european-union).

These capabilities will be used again later in this report (PART III) to illustrate potential advantages and limitations of various approaches to bolstering EU cyber defence capabilities.

3.3.1 Detection capabilities

Detection capabilities can take many forms, ranging from passive perimeter monitoring to active within-network monitoring. However, whatever specific form it takes, detecting a cyber incident is critical for both withstanding and preventing a cyberattack.

In the event of an incident, detection is the first step in effective and efficient incident response. Some methods for detection fall under security measures, such as firewalls and malware detection software. Detection also plays an important role in triggering processes geared towards resiliency, such as limiting access to other systems, reporting incidents to government or EU agencies, and coordinating responses with other firms. Any crisis response – whether it be with an in-house team, a sectoral or a national Computer Emergency Response Team (CERT), or an EU agency such as ENISA – begins with detection.

Detection capabilities are also an important component of prevention. Specifically, detection capabilities form a core component of strategies to deter through punishment and denial as well as dissuade through norms/taboos. In order to punish, the target must attribute the incident to a specific actor. Yet, in order to attribute, the target first has to know that an incident has occurred. Detection represents a similarly critical step for denial-based deterrence approaches, since it forms a first step in both security and resilience measures. Finally, detection capabilities are also essential for efforts to dissuade a potential aggressor through the use of norms/taboos. In order for the international community to impose reputational costs for certain types of behaviour, actors need to be able to observe when a specific norm is broken and by whom.

3.3.2 Attribution capabilities

Attribution builds upon the prior capability – detection – by assigning responsibility for a specific incident or set of incidents. There are three broad categories of attribution, each of which serves a distinct purpose: technical, political, and legal. Technical attribution consists of cyber forensics. It may identify a specific group or actors but it does not assign political or legal responsibility. Political attribution is the process through which policy elites assign responsibility for an attack for strategic or political purposes (e.g. to deter through punishment or to dissuade through norms/taboos). This process is supported by technical attribution, but may be aided by national intelligence

efforts and is driven by political and strategic concerns.[76] Finally, legal attribution hinges on the standard needed to impose legal consequences on hostile actors. This process may rely on technical attribution or national intelligence, but the assigning of responsibility has to hold up to public, legal scrutiny. For this Task Force, we are most concerned with technical and political attribution, although legal attribution can be used to impose costs on hostile actors through international and domestic law. Cybercrime, in contrast to cyber defence, would be most concerned with technical and legal attribution.

Attribution (technical and political) forms a central component of two prevention-based cyber defence strategies: punishment and norms/taboos. Both hinge on imposing costs in direct response to an incident. In order to impose costs, the target must first be able to identify at a political level who is responsible.

Notably, political attribution is not necessary for denial or entanglement approaches to prevention or to security and resilience efforts in order to withstand an attack. Technical attribution, however, remains a core component of denial and preparedness strategies. Understanding the who, what, when, where, and how of an incident is useful for improving upon security and resilience measures in the future. Why an incident occurred (understanding the motivation behind an attack) is politically important but not essential for bolstering security or resilience measures.

3.3.3 Incident response capabilities

Both preventing an attack through denial and withstanding an attack if prevention fails hinges on the sophistication of incident response capabilities. Incident response capabilities pull together technology and processes in order to react to an incident in real time. It requires the ability to cooperate quickly, across borders, agencies, and institutions both horizontally (within the sector, domestic government, or the EU) and vertically (between firms and the government or the government and the EU).

In order to be effective in times of crisis, incident response models need to be put into place prior to a crisis. Preparedness is cemented through various governance models, which provide specific mandates to various actors and either institutionalise or informally familiarise stakeholders with procedures for detection, denial, and recovery. As such, these governance models may contain regulations and standards setting, facilitate a variety of information sharing opportunities, coordinate incident response teams and procedures, connect

[76] It is worth noting that political or legal attribution may play an important role domestically independent of a specific cyber defence strategy. Citizens expect to know who was responsible and what the government is doing in an effort to secure their interests.

communities of practice with policy bodies, and clarify command and communication procedures in the event of an incident. Ideally, research and development would provide a strong technical foundation upon which security and resilience can be built. Moreover, specific challenges to these cyber security and resilience models would have undergone fine tuning and, given that cyber defence faces both a command and a communications challenge,[77] would have become familiar to all levels of the chain of command through exercises and skills trainings for CERTs.

3.4 Concluding thoughts: threats and defence

In conclusion, this rapidly evolving threat space has negatively impacted and will continue to negatively impact the EU and its member states.

In order to bolster its cyber defence capabilities, the EU has a range of strategies at its disposal focusing on preventing – deterrence and dissuasion – and withstanding – security and resilience – cyber incidents. These cyber defence strategies face unique operational challenges and depend on specific tactical and operational capabilities, such as detection, attribution, and incident response.

Finally, it is important to note that these strategies and operations should not occur in isolation but rather as complementary components within an overarching defence posture. Some of these strategies – denial-based deterrence and security and resilience, for example – rely on heavily overlapping tactical and operational capabilities.

[77] There are two levels of action in cyber defence: (i) technical operators and (ii) policy bodies. At the operator level, things are done at a scale of minutes to hours because they are discrete technical tasks. However, when you start to elevate something to the level of a national or EU incident, say an attack on critical infrastructure, then policy bodies begin to become involved. With these two levels of action, there are both command and communications challenges in cyber defence: how to communicate tasks and priorities laterally (across technical teams, operator level, watch officers, etc.) but also vertically (up and down the chain of command). This is both a communications challenge and a time domain challenge given that the tempo at which executives and high level political leaders operate is often very different than the tempo for operators.

PART II
THE STATE OF PLAY AND THE CASE FOR GREATER COOPERATION

4. THE NEED FOR A NEW EU-WIDE RESPONSE

Given the realities of the threat space and potential defence strategic and operational capabilities, greater coordination and cooperation would prove advantageous. This section of the report will illustrate this with an analysis of the need for greater EU coordination in cyber defence. It includes a breakdown of the advantages of coordination in cyber defence, the case for coordination across the EU, a discussion of the evolution of EU Cyber Defence Policy, and an overview of the current institutional EU framework and its shortcomings.

4.1 The advantages of coordination

The benefit of cooperation and coordination between EU member states in order to increase cyber defence capabilities is threefold.

4.1.1 Structure of cyberspace

First, coordination is well suited to the structural realities of cyberspace. Cyberspace is global and remains significantly unbounded by territorial boundaries, readily crossing national borders. Activity inevitably passes through a host of national jurisdictions on its route from endpoint to endpoint. Hostile or malicious activity is no exception. Botnets,[78] for example, leverage a collection of compromised computers, servers, and increasingly IoT devices, which can be located anywhere in the world, to attack a target system.

The infrastructure required to respond to these types of activity, are likewise often found outside the territory of the target of malicious activity. Take for example the 2007 DDoS attack against Estonia that effectively overwhelmed servers and shut down financial, media, and telecommunications services as well as government websites and communication networks.[79] In response to

[78] Botnets can be leveraged to carry out a range of malicious activity such as DDoS attacks and information theft.

[79] For additional information on the Estonia 2007 events refer to an analytical overview of the events from Davis, Joshua (2007), "Hackers Take Down the Most Wired Country in the World", *Wired Magazine*, 21 August (https://www.wired.com/2007/08/ff-estonia/) and The

internet traffic flooding in from around the world, the decision was made to cut Estonia off from outside traffic. However, this required cooperation from Sweden, whose servers were required to sever Estonia's international connection.

4.1.2 Critical services and infrastructure

Second, coordination is well suited to the structural realities of essential services and critical infrastructure within the EU and its member states, which are increasingly interconnected.[80] Countries have cross-border dependencies and interdependencies within critical services and sectors (e.g. water distribution or sanitation in one country being reliant on an energy grid in a neighbouring country or energy providers operating across a suite of countries), which can be sectoral or geographic in nature.[81] This can result in cascading outages or contagion across systems that span national borders in the event of a cyber incident.

Moreover, EU institutions and critical functions are by design supra-national or inter-governmental in nature. This includes institutions like the European Commission and its Directorates-General (DGs), the European Central Bank (ECB), and the European External Action Service (EEAS) as well as services such as the recently launched Galileo – the European Union's Global Satellite Navigation System (GNSS). Cooperative security and resilience efforts are likewise needed to address the cyber defence of the EU itself.

As a consequence of the structural reality of critical services and infrastructure within the EU, the resources needed to deploy in order to detect, deny, and recover from cyber incidents within the EU largely lie in more than

---

Swedish Management Agency (2008), "Large scale Internet attacks: The Internet attacks on Estonia and Sweden's emergency preparedness for Internet attacks", *SEMA´s Educational Series*, Issue 2 (https://www.msb.se/RibData/Filer/pdf/26164.pdf). For an overview of the events as related to the current state of affairs refer to Tamkin, Emily (2017), "10 Years After the Landmark Attack on Estonia, Is the World Better Prepared for Cyber Threats?", *Foreign Policy*, 27 April (https://foreignpolicy.com/2017/04/27/10-years-after-the-landmark-attack-on-estonia-is-the-world-better-prepared-for-cyber-threats/).

[80] See, for a more detailed definition of critical infrastructure protection, Haemmerli and Renda (2010), Protecting Critical Infrastructure in the EU, Report of a CEPS Task Force, CEPS.

[81] Interdependency and dependency in the context of critical infrastructure and services is a widely acknowledged issue. For examples of research focusing on modelling these dependencies, refer to Zimmerman, R., Restrepo, C. (2006), "The next step: Quantifying infrastructure interdependencies to improve security", *International Journal of Critical Infrastructures* 2(2-3); Luiijf, Eric et. al. (2010), "Empirical findings on European critical infrastructure dependencies", *International Journal of System of Systems Engineering* 2(1); and Nguyen, Tri-Dung et. al. (2016), "Modelling infrastructure interdependencies, resiliency and sustainability", *International Journal of Critical Infrastructures* 12(1/2).

any one single EU member state, outside the military or defence organisations, and even outside the public sector itself. As a result, cyber defence, in its most robust form, necessitates cross border, civilian-military, and public-private interplay.

4.1.3 Pooling of resources

Third, coordination allows for the pooling of resources, either through the creation of new tools through joint investment or through the provision of assistance using existing national tools. The threat space is vast and individual states only have a limited set of resources at their disposal. Pooling allows those resources to be amplified and offer the potential for greater investment in resilience and security measures. In addition, given the importance of situational awareness in deploying deterrence and/or preparedness strategies, states would benefit from the greatest scope and granularity of information and analysis possible.

In addition, coordination already occurs among malicious actors, often not through pooling of resources, but because of the shared intent of causing damage to some company, institution or group. The answer to a coordinated attack must also be coordinated.

4.2 The case for coordination at the EU level

Given the clear benefits of coordination, what then is the EU's added value in cyber defence? The functions of the EU are well suited to cooperative responses. The three broad benefits discussed in the previous sub-section all point to clear advantages of greater coordination and cooperation in cyber defence. The EU is a core institutional mechanism for facilitating coordination and cooperation in Europe. In the most general sense, the EU's added value in any space is through coordination and cooperation between states; harmonisation of policies and agendas; and pooling or aggregation of resources, capabilities, and responsibilities between previously disparate actors.

Moreover, coordination in cybersecurity and defence requires building and maintaining trust. Trust can occur at three levels: peer-to-peer (person to person), among those in command (trust in a principal or institution), and/or built into the system in terms of design (e.g. blockchain). The first two avenues for trust can be built and maintained, in part, through shared interests, exercises, clear regulations and enforcement, standard operating procedures, and demonstrated efficiency and efficacy. While there is no single avenue for the creation of trust, consistent and frequent cooperation, which is already found in the EU, is a helpful foundation upon which to build.

The question then becomes, what specific configurations of these broader activities will provide the greatest cyber defence capabilities for EU institutions and for EU member states? While the EU is a fairly acceptable and tested coordinating mechanism, in cyber defence, speed and complexity are high and create significant challenges for the EU's standard security and crisis conflict mechanisms.

4.3 The rise of EU cyber defence policy

With the European Cybersecurity Strategy of 2013, the EU started to implement concrete policies to create cyber defence capabilities in the EU. One of the five strategic priorities set in February 2013 was indeed to develop cyber defence policy and capabilities related to the framework of the CSDP. The EU started to realise the need to focus cyber defence capabilities on detection, response, and recovery from sophisticated cyber threats and to promote coordination between civilian and military actors in the EU and at the international level with partners such as NATO and other international organisations.[82]

Also of note in 2013, the Heads of State and Government in their conclusions of the European Council acknowledged cyber as one out of four key capability shortfalls in the EU and called on the EDA to act in order to address this shortfall. At the policy level they also called for an EU Cyber Defence Policy Framework, on the basis of a proposal by the High Representative, in cooperation with the Commission and the EDA. The EU Cyber Defence Policy Framework was endorsed in 2014 and became the reference policy document on cyber defence. Based on the experience gained from the implementation and the developments regarding EU security and defence in the implementation of the Global Strategy, the European Council called for an updated version of the Cyber Defence Policy Framework, which will be completed by the end of 2018.

However, it was only in 2016 that EU-NATO collaboration started to take shape. At the summit in Warsaw, the Presidents of the European Council and the European Commission, and the NATO's Secretary General signed a joint declaration signalling greater security cooperation between the two institutions. The Joint Declaration emphasised seven categories for cooperation between NATO and the EU. Two were directly applicable to cyber defence: countering hybrid threats and cyber security and defence.[83] The joint declaration reaffirmed

---

[82] European Commission (2013), *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace,* Brussels.

[83] European Union External Action Service "EU-NATO cooperation – Factsheet" (https://eeas.europa.eu/headquarters/headquarters-Homepage/28286/eu-nato-cooperation-factsheet_en).

the importance of EU-NATO coordination in security, and in cybersecurity more specifically. The core mandates of both institutions differ and could provide interlocking or complementary functions in increasing European cyber defence capabilities.

Cyber defence was also pursued in 2017 under the Permanent Structured Cooperation (PESCO) framework,[84] although participation is voluntary and not EU-wide.[85] Two current PESCO projects specifically focusing on cybersecurity concerns explicitly illustrate a persistent demand for tactical and operational solutions to cybersecurity challenges. The first project, "Cyber Rapid Response Teams and Mutual Assistance in Cyber Security", centres on three opportunities for coordination and cooperation that the EU is not currently pursuing – penetration testing, joint capabilities, and mutual operational support – through the creation of specific Cyber Rapid Response Teams.[86] The second project, "Cyber Threats and Incident Response Information Sharing Platform", centres on increasing situational awareness and creating solutions for intelligence sharing that are easier to access than those currently in use by intelligence services and various technical communities.[87] Although neither of these projects are EU-wide and they do not address the full spectrum of cyber defence strategies from deterrence to preparedness, both PESCO projects focus on areas where inter-state coordination and the pooling of resources would increase state resiliency to and crisis management of cyberattacks. Although each of these projects fall short of the EU-wide response called for in this report, both illustrate the operational and tactical concerns facing member states and the demand by many states to meet these challenges more effectively through deeper coordination.

---

[84] High Representative and Vice-President Federica Mogherini gave the following description of PESCO in December 2017: "We have activated a Permanent Structured Cooperation on Defence – ambitious and inclusive. 25 Member States have committed to join forces on a regular basis, to do things together, spend together, invest together, buy together, act together. The possibilities of the Permanent Structured Cooperation are immense." For additional information on PESCO, refer to the "Permanent Structured Cooperation (PESCO) – Factsheet" (https://eeas.europa.eu/headquarters/headquarters-Homepage/34226/permanent-structured-cooperation-pesco-factsheet_en).

[85] See Blockmans, S. (2017), "Europe's defence train has left the station—Speed and destination unknown", CEPS Commentary, 12 December, Brussels.

[86] So far, this PESCO project has seven participating states (Croatia, Finland, France, Lithuania (lead country), the Netherlands, Romania, and Spain) and five observing states (Belgium, Estonia, Germany, Greece, and Slovenia).

[87] So far, this PESCO project has eight participating states (Bosnia, Cyprus, Greece (lead state), Hungary, Italy, Ireland, Portugal, and Spain) and seven observing states (Belgium, Denmark, Estonia, Finland, Lithuania, and Slovenia).

In September 2017, the European Commission and the High Representative of the Union for Foreign Affairs and Security Policy, reaffirmed with a joint communication (introducing a multi-element cybersecurity effort referred to as the 2017 Cybersecurity Package) to the European Parliament and the Council, the commitment to cyber defence, strengthening EU-NATO cooperation in countering hybrid threats and improving communications between all relevant institutions including ENISA.[88]

It is also important to mention the recent motion from the European Parliament on Cyber Defence approved on 25 May 2018. It emphasises that "while cyber defence remains a core competence of member states, the EU has a vital role to play in providing a platform for European Cooperation […] and that whereas current vulnerability is due mainly to the fragmentation of European defence strategies and capabilities, […] much more needs to be done as it is becoming more and more difficult to counter cyber-attack at member states level, […] whereas cyber defence and deterrence are activities that can best be tackled cooperatively at European level".[89]

In the context of reinforcing cybersecurity technological capacity, it is also helpful to note the recent proposal from the European Commission for a Regulation of the European Parliament and the Council establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres. One of the goals envisaged by this proposal is also to enhance synergies between the civilian and military dimensions of cybersecurity to increase cooperation between civilian and defence cybersecurity research and innovation communities.[90]

Finally, the solidarity and self-defence clauses of the Treaty on the European Union (TEU) provide two additional EU institutional avenues for addressing cyber incidents. After all, one could take the view that cyberattacks, used as weapons with the aim of causing severe damage and disruption to a member state and identified as coming from an external entity, could qualify as 'armed aggression' in the sense of Article 42(7) TEU, which is commonly

---

[88] European Commission (2017), Joint Communication to The European Parliament and The Council, Resilience, Deterrence and Defence: Building strong cybersecurity for the EU, JOIN/2017/0450 final.

[89] European Parliament's Committee on Foreign Affairs (2018), "Report on Cyber Defence". Plenary Session. 25 May, p. 5.

[90] European Commission (2018), "Proposal for a Regulation of the European Parliament and the Council establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres" (https://ec.europa.eu/digital-single-market/en/news/proposal-regulation-establishing-european-cybersecurity-industrial-technology-and-research).

referred to as the EU's mutual assistance clause, if the member state's security is significantly threatened by its consequences. This provision reads as follows:

> If a member state is the victim of armed aggression on its territory, the other member states shall have towards it an obligation of aid and assistance by all the means in their power, in accordance with Article 51 of the United Nations Charter. This shall not prejudice the specific character of the security and defence policy of certain member states.
>
> Commitments and cooperation in this area shall be consistent with commitments under the North Atlantic Treaty Organisation, which, for those States which are members of it, remains the foundation of their collective defence and the forum for its implementation.[91]

In cases where a 'threat agent' is unclear, reference could be made to Article 222 TFEU, known as the 'solidarity clause', for preparing an EU-wide disaster response.[92] In fact, the solidarity clause rests at the centre of the proposed crisis response blueprint as part of the Commission's 2017 Cyber Security Package (this proposal is discussed in more detail in the conclusion of this section and in the discussion of Scenario I in the following section). "The blueprint complements existing EU crisis management mechanisms, adding procedures for a cybersecurity dimension, as a major cyber incident could provide the basis for member states to invoke the EU 'Solidarity Clause' (Article 222 TFEU)."[93] While the EU's mutual assistance clause would place any EU action within the context of armed aggression, the EU's solidarity clause would place it in the context of disaster response.

4.4 The current EU approach and ecosystem

Although the EU has made progress in addressing cyber defence in recent years, its cyber defence capacity remains largely fragmented across, and siloed within, various institutions, agencies, and initiatives. Moreover, there is no standing model for or independent power to respond to cyberattacks at the EU level. While EU institutions have been tasked with the provision of expertise or advice, the operational and strategic realities of cyber defence remain located within member states.

---

[91] For a more detailed analysis of Article 42(7) TEU and its historical invocations refer to Christophe Hillion and Steven Blockmans (2015), "Europe's self-defence: Tous pour un et un pour tous?", CEPS Commentary, 20 November.

[92] EUISS Yearbook of European Security 2018, pp. 122-3

[93] Ibid, p. 170.

This sub-section proceeds in two parts – (i) an overview of tactical and operational versus strategic or policy mechanisms for crisis response and preparedness and (ii) an overview of the internal versus external security frameworks for cyber defence – before concluding with a review of the shortcomings of the existing cyber defence architecture.[94]

4.4.1 Communities of Practice versus Policy Mechanisms

In terms of crisis preparation and crisis response, preparedness (i.e. security and resilience) occurs at two levels: at the tactical and operator level and then at the strategic or policy elite level. Each of these levels of action face different sets of tasks and concerns. For example, operators are concerned with discrete technical tasks and processes, while policy elites are concerned with questions of punishment, attribution, or conflict escalation.

Operators and Communities of Practice

Communities of practice focus primarily on the tactical and operational levels of cyber defence, leaving the strategic dynamics to security and policy bodies. These practitioners (technical first responders, systems operators, and operational advisors) are grouped into two organisations within the EU: ENISA and CERTs. In addition, the European Directive on Security of Network and Information Systems (NIS Directive) focuses on member states' operational cyber defence capabilities.

ENISA refers to itself as "the centre of expertise for cyber security in Europe".[95] Located in Greece, it serves as a centre for enhancing network and information security within the EU through operational support. However, it is important to note that its role is solely supportive in nature. Operational cyber defence, in practice and on paper, remains the purview of member states. ENISA, in contrast, raises awareness, supports policy development, and facilitates capacity building at the EU and state level.

---

[94] For an alternative analytic framing the EU approach to cyber security, refer to the European Political Strategy Centre (EPSC)'s 2017 report, "Building an Effective European Cyber Shield: Taking EU Cooperation to the Next Level". They refer to the institutionalisation of cybersecurity as centred around "four different constituencies", which are "currently engaged in cybersecurity at European level, respectively covering IT security; law enforcement; intelligence; and diplomacy and defence-related aspects" (p. 7). These categories closely complement those in this report (http://ec.europa.eu/epsc/sites/epsc/files/strategic_note_issue_24.pdf).

[95] The European Union Agency for Network and Information Security, "About ENISA". Accessed July 1, 2018 (https://www.enisa.europa.eu/about-enisa).

The first responders in cyber defence are primarily located within CERTs or Computer Security Incident Response Teams (CSIRTs).[96] For the EU, these first responders are located in CERT-EU, which focuses on providing tactical and operational assistance to EU institutions.[97] At the national level, the structure of these CERTs diverges significantly both in form and function. In each state, there can be a number of CERTs ranging from companies, banks, regional governments, national governments, etc. There is also wide variance in capability between member states, which is evidenced by limited membership in the selective European Government CERTs (EGC) group.[98] Alongside CERT-EU, there are only ten national CERTs in its ranks.[99] Trust remains a central rationale for maintaining this limited membership. As a self-described "operational group with a technical focus", the EGC serves to foster cooperation between governmental CERTs in Europe.[100] In addition to the EGC, international CERT cooperation occurs through the CSIRT Network (both CERT-EU and ENISA are members), a task force aimed at cooperation in Europe and neighbouring regions (TF-CSIRT)[101], and globally through entities such as the Forum of Incident Response and Security Teams (FIRST).[102]

The EU's first piece of cybersecurity legislation, the European Directive on Security of Network and Information Systems (NIS Directive), also sits within the operational space. However, this EU directive focuses on developing capabilities within member states themselves rather than at the EU level. Recognising that cyber preparedness varies significantly between all 28 EU

---

[96] European Political Strategy Centre (2017), "Building an Effective European Cyber Shield: Taking EU Cooperation to the Next Level", *EPSC Strategic Notes*, Issue 24. 8 May: p. 7 (http://ec.europa.eu/epsc/sites/epsc/files/strategic_note_issue_24.pdf).

[97] For more information on CERT-EU, visit their webpage at https://cert.europa.eu/cert/filteredition/en/CERT-LatestNews.html.

[98] The EGC has limited membership with high standards for entry. Its webpage, as of spring 2018, indicates that applications are now closed. Given its restrictive community and the corresponding levels of trust, the EGC is an important avenue for information sharing and incident response cooperation for its members.

[99] Alongside CERT-EU, the following CERTs are members of the EGC: Austria's GovCERT Austria, Belgium's CERT.be, Denmark's CFCS-DK, Finland's NCSC-FI, France's CERT-FR, Germany's CERT-Bund, Netherlands' NCSC-NL, Norway's NorCERT, Spain's CCN-CERT, Sweden's CERT-SE, Switzerland's GovCERT.ch, United Kingdom's CERT-UK, and United Kingdom's GovCertUK.

[100] European Government CERTs (EGC) group webpage. Accessed June 20, 2017 (http://www.egc-group.org/).

[101] For more information on TF-CSIRT, visit their webpage at https://tf-csirt.org/tf-csirt/.

[102] For more information on FIRST, visit their webpage at https://www.first.org/.

member states, the NIS Directive serves as a corrective by setting certain institutional requirements for all states (such as the creation of a national CSIRT and the creation of a domestic NIS authority). It also requires states to identify their own domestic critical sectors and infrastructure, which will now need to report serious incidents to a relevant national authority.[103] The NIS Directive came into force on May 9, 2018.

Policy Mechanisms for Crisis Response

At present, there is no self-standing policy mechanism for responding to cyberattacks on or within the EU. However, there are two potential policy venues that may be leveraged to respond to an emerging cyber crisis: the Integrated Political Crisis Response (IPCR) and the Cyber Diplomatic Toolbox.

One possible avenue would be to use the IPCR, which was adopted in 2013 in an attempt to address risks and impacts that increasingly span borders and sectors without replacing existing sectoral arrangements or member state responsibilities. With this in mind, IPCR was based on existing Council procedures, placed under the political control and strategic direction of the Presidency, and organised around COREPER. The IPCR process follows four broad stages – situational awareness, prioritisation of risks, formulation of strategies, and implementation of strategies – which allows it to be flexible and scalable between different types of crises. Two of its strengths, therefore, are that its Roundtable can bring a variety of actors to the table in various configurations and its weekly Integrated Situational Awareness and Analysis (ISAA) reports combine information from national sources related to a crisis into one single analytical document. So far, the IPCR has only been invoked once (for the migration crisis). However, it has also carried out a series of exercises including one cyber security specific exercise.

In addition to the potential crisis response mechanism of the IPCR, in 2017 the Council of the European Union launched the "Cyber Diplomatic Toolbox". This initiative sought to build out a framework for joint EU diplomatic action in an effort to both deter and respond to cyber crises. This toolbox resides within the Common Foreign and Security Policy (CFSP), which is housed within the EEAS. Sico van der Meer, a research fellow at the Netherlands Institute of International Relations, argues that "as member states invest in developing defensive and offensive cyber capabilities both for their own protection and within NATO, the proposed toolbox is an attempt to balance their emerging

[103] Additional NIS Directive requirements can be found on the European Commission's website at https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive.

hard power capabilities with collective soft-power measures."[104] Notably, however, this initiative is still in its infancy and protocols for how and when it would be deployed have yet to be fully developed or formalised.

Ultimately, as it stands now, the model for crisis response spanning policy elites and operators would need to largely unfold alongside the crisis itself. The aim would be to quickly reach an agreement at the elite level while operators troubleshoot in real time and then define the operational protocols, decide who initiates the response, who monitors the response, etc. For instance, if the attack targets hospitals, then the response will focus on DG SANTE from the Commission, which in turn would work with ENISA, the CSIRT networks, and national governments and their suite of CERTs and the healthcare industry. The exact configuration would unfold in real time.

4.4.2 Internal versus External Security Institutionalisation

Within security policy more generally, a common division occurs between internal security (law enforcement) and external security (defence and diplomacy). The EU's approach to cyber defence, as of yet, is no exception. Importantly, in practice, cyber defence often blurs internal and external security boundaries, sometimes challenging the conceptual boundaries between criminal activity and state sponsored aggression (or conflict) and intelligence gathering efforts. Interconnected networks, widely available tools, and hybrid warfare are all elements that contribute to make the line between internal and external quite grey. Moreover, the core responsibilities primarily lie with the member states themselves while EU institutions assist, advise, facilitate and support, etc.

Internal Security and Law Enforcement

Europol remains the primary internal security and law enforcement institution with a mandate for cybersecurity in a broader sense. Established in 2013, their European Cybercrime Centre (EC3) serves to strengthen cybercrime response within the EU through a focus on cyber law enforcement operations. More specifically, it facilitates information exchange, conducts forensic analysis, provides intelligence, and offers legal assistance. EC3 also houses the Joint Cybercrime Action Taskforce (J-Cat).[105]

---

[104] van der Meer, Sico (2017), "EU Creates a Diplomatic Toolbox to Deter Cyberattacks", The Council of Foreign Relations' *Net Politics* and *Digital and Cyberspace Policy Program*, 20 June (https://www.cfr.org/blog/eu-creates-diplomatic-toolbox-deter-cyberattacks).

[105] For additional information on EC3 and J-Cat refer to their webpage: https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3.

External Security and Diplomacy

Under the EEAS, which serves as the EU's diplomatic service, there are three small teams of note. First, the Intelligence Centre (INTCEN) serves as the intelligence body of the EU. Notably, most cyber intelligence capacity and activity occurs within national intelligence agencies. Second, the EEAS has a small team focusing on diplomatic responses to coercive cyber operations from state or non-state actors. Third, also under the EEAS, a small EUMS (EU Military Staff) team seeks to integrate cyber defence into CSDP operations and missions.[106]

Under the EDA, which focuses on capability development through cooperation between member states, a small team supports specific cyber defence capability integration and development.[107] Again, this team's mission, like the EDA itself, is to assist member states with the development of their capabilities through cooperation and to identify gaps in member state capabilities rather than to build out a specific EU-level defence capacity in this space. The development of capabilities follows the prioritisation process of the Capability Development Plan which is the key reference on capability development for national and multinational action including as regards the EU security and defence initiatives such as PESCO and the European Defence Fund.

Cyber defence has also been pursued under PESCO framework and the joint EU-NATO 2016 joint-declaration in Warsaw, both of which were discussed in more detail during the previous section dedicated to the evolution of cyber policy within the EU.

4.5 Limitations to the current EU cyber defence posture

4.5.1 An advisor, not an actor

The EU plays a largely advisory role in cyber defence, which has yet to be fully implemented, leaving the operational and strategic realities of defence to the member states. Yet, these strategic and operational realities form the backbone of cyber defence. As such, the EU's current approach is to support member states in the implementation of their individual strategies and operations rather than build out and maintain a defence posture of its own. Although, it is important to mention that here as well, the EU plays an important role, as in many domains, as a regulator and a law-maker.

---

[106] European Political Strategy Centre (2017), "Building an Effective European Cyber Shield: Taking EU Cooperation to the Next Level", *EPSC Strategic Notes*, Issue 24. 8 May: p. 7 (http://ec.europa.eu/epsc/sites/epsc/files/strategic_note_issue_24.pdf).

[107] Ibid.

4.5.2 *A fragmented approach, lacking a strategic vision*

The EU approach remains highly fragmented across a variety of dimensions – internal versus external security and operators versus policy elites – as well as within each of these dimensions.

There are three important outcomes of this fragmentation:

1. The EU lacks a cohesive strategic vision for and oversight over cyber defence efforts.
2. The EU lacks a cohesive or streamlined mechanism needed for real time crisis response in complex situations.
3. Barriers between the EU's various actors are often quite high with horizontal cooperation and information exchange between them limited.
4. Barriers between member states and these EU institutions have also proved to be fairly rigid with need for greater vertical cooperation.

The above task of mapping out the relevant actors and institutional structures operating within the EU illustrates the fragmentation, gaps in coverage, and sometimes unknowing duplication of capabilities and mandates. The complexity of the institutional arrangement leaves operators and policy practitioners, as well as internal and external security actors, largely uncertain of the broader EU cyber defence posture, its institutional hierarchies and division of labour in times of peace and in times of crisis.

4.5.3 *Lack of resources*

Fragmentation is accompanied by serious concerns over staffing and resources at the EU level. For example, EC3 requires significant additional funds to continue its successful track record on cybercrime. It currently has a staff of 52 people.[108] The EEAS and EDA combined currently have 12 people focusing on this area, while ENISA has a staff of 65 and CERT-EU has a staff of 30.[109] In all of these five organisations combined, the EU has a staff of 159 individuals tasked with cyber security.

To put this in perspective, by the end of 2017, the staff of just one of the institutions tasked with cyber security and defence in the US – the US Cyber Command's (USCYBERCOM) Cyber National Mission Force Headquarters (CNMF-HQ) – had grown to approximately 1,900 according to publicly available sources.[110] The corresponding 133 Cyber Mission Force (CMF) teams had

---

[108] Ibid.

[109] Ibid.

[110] US Cyber Command (https://www.cybercom.mil/About/History/).

approximately 5,000 personnel between them as of October 2016.[111] This number was projected to grow to approximately 6,200 by the end of 2018.[112]

It must not be forgotten that cyberspace underpins the daily functioning of critical infrastructure and essential services, national governments and EU institutions, as well as being vital to the military and business. The scope is broad and the level of complexity high. Presently, the resources allocated by the EU are neither commensurate to this scope or adequate for this level of complexity.

4.6 Concluding thoughts: an urgent need

At present, the EU lacks a cohesive vision or strategy for cyber defence, core competencies and capabilities remain in the hands of member states, and EU capabilities remain siloed and under-resourced.

Given the limitations of the current EU approach, concern over the readiness of the EU to weather cyber incidents have been raised throughout its various institutions. President Jean-Claude Juncker argued in his 2017 State of the Union address that although the EU has "made progress in keeping Europeans safe online", "Europe is still not well equipped when it comes to cyberattacks."[113] This was further reinforced in the European Parliament with the 2018 Committee on Foreign Affairs report on cyber defence, which recognised that "while cyber defence remains a core competence of the member states, the EU has a vital role to play in providing a platform for European cooperation, and in ensuring that these new endeavours are closely coordinated at an international level and within the transatlantic security architecture from the start, to avoid gaps and inefficiencies that mark many traditional defence efforts."[114]

Calls for greater cooperation and coordination abound, but the specific potential configurations of that cooperation and coordination at the EU level remain, arguably, underdeveloped. That said, there are efforts currently to reform or improve the existing fragmented cyber defence environment, such as the Commission's 2017 Cyber Security Package, which is currently progressing through co-decision and is expected to be implemented (as of 8 September, 2018

---

[111] Ibid.

[112] Ibid.

[113] European Commission (2017), "State of the Union 2017 - Cybersecurity: Commission scales up EU's response to cyber-attacks", Press Release, 19 September (http://europa.eu/rapid/press-release_IP-17-3193_en.htm).

[114] European Parliament's Committee on Foreign Affairs (2018), "Report on Cyber Defence". Plenary Session, 25 May, p. 5.

it had entered Trilogue negotiations), for the most part in its current form.[115] Notably, this effort forms the backbone of Scenario I: the Base Case Scenario discussed in more detail in the next section of this report.

[115] For more information on the 2017 Cyber Security Package, refer to the European Commission's webpage https://ec.europa.eu/info/law/better-regulation/initiatives/com-2017-477_en and to the European Parliament's September 2018 briefing http://www.europarl.europa.eu/RegData/etudes/BRIE/2017/614643/EPRS_BRI(2017)614643_EN.pdf.

PART III
BOLSTERING EU CYBER DEFENCE

5. THREE PATHS FORWARD

5.1 Introduction

Given the threats facing the EU, the advantages of cooperation, and the limitations of the current EU approach to cyber defence, this Task Force developed three scenarios for strengthening EU cyber defence capabilities.[116]

The three scenarios are as follows:

I. The Base Case: implementing the 2017 Cyber Security Package
II. Establishing a Cyber Defence Coordinator
III. Creating a Cyber Defence Agency

Each of these scenarios builds directly on current EU capabilities and institutions as well as on the scenario(s) preceding them. To that end, these three scenarios represent an iterative progression beginning with the state of play, passing through the 2017 Cyber Security Package and the creation of a Cyber Defence Coordinator, and concluding with the creation of a Cyber Defence Agency.

In summary, Scenario I entails an increase in operational cyber defence capabilities, although it maintains the EU's largely advisory role with the bulk of cyber strategy and operations remaining in the hands of member states. It also enables the full implementation of the current cyber defence approach, which so far has remained partially incomplete. The overall structure/institutionalisation of defence capabilities remains largely consistent with the current state of play.

Scenario II takes the increased advisory capacity developed in Scenario I and adds an upper layer of oversight and coordination. Since the coordinator cannot set policy, the strategic and operational realities of cyber defence would continue to remain primarily with the member states. However, the coordinator could serve to partially break down silos and address fragmentation. A coordinator can also better address resource needs and allocation.

Scenario III expands the existing EU advisor capabilities found in Scenarios I and II while simultaneously adding a strategic and operational mandate at the EU level. The creation of an agency allows for the oversight function of the coordinator in Scenario II but also the joint development of and

[116] Note: not all participants contributed to the development of the scenarios.

cooperation towards EU detection, attribution, and incident response capabilities. The agency can also address resource allocation more effectively and efficiently.

5.2 Building off current EU capabilities

This section of the report will provide an overview of each scenario including a summary of their organisation and core activities followed by a discussion of the strengths and weaknesses of each in relation to the goal of bolstering EU cyber defence capabilities.

5.2.1 Scenario I - The Base Case: Implementing the 2017 Cyber Security Package

Scenario I assumes the approval of the Commission's 2017 Cyber Security Package, which is currently progressing through co-decision but is expected to be implemented within the year with only minor revisions to content (as of September 8th, 2018 it had entered Trilogue negotiations).[117] The Cyber Security Package would augment the current state of play through the implementation of four basic measures:

1. strengthening ENISA,
2. implementing the NIS Directive,
3. creating a Cybersecurity Emergency Response Fund, and
4. increasing resilience through rapid emergency response procedures.

Given the limitations of the EU's current approach to cyber defence, full implementation of Scenario I would address in part concerns around (i) the advisory role of the EU, (ii) the negative consequences of fragmentation, and (iii) the persistent lack of resources.

Advisory Role

First, Scenario I would strengthen the EU's advisory role by increasing the mandate of ENISA and continuing to implement previous cyber defence initiatives such as the NIS Directive. Under the Cybersecurity Package, ENISA's cyber defence capabilities would include:

- Supporting and contributing to EU efforts in cybersecurity in full cooperation with EU institutions.

[117] For updates on the legislative progress of the Cybersecurity Package, visit the European Parliament's website at http://www.europarl.europa.eu/legislative-train/theme-connected-digital-single-market/file-cyber-security-package.

- Assisting the Commission by advising on cybersecurity policy and capacity development.
- Promoting the implementation of the NIS Directive.
- Assisting member states in building capabilities and preparedness to prevent, detect, and respond to cyber threats. In particular, ENISA should promote the development of national CERTs.
- Supporting information sharing by providing best practices and guidance on how to address regulatory issues.
- Contributing to an EU level of response.
- Making use of the technical expertise found in CERT-EU.
- Collecting relevant, publicly available intelligence.

However, Scenario I would continue to place the EU in an advisory role with the strategic and operational realties of cyber defence remaining with member states. This is evident both in the tasks assigned to ENISA and in the limitations placed on ENISA. The EU will support, contribute, assist, and promote. Moreover, the EU (through ENISA), should not supersede states. Its actions should solely be complementary to the actions taken by member states.

While there is a deepening of the advisory and support-based role of the EU, implementation of the Cyber Security Package would not radically increase the strategic or operational cyber defence capabilities of the EU itself.

Fragmentation

Second, with the Commission's recommendation of a Blueprint for crisis response, Scenario I would mitigate, in part, the negative impact of fragmentation on crisis response. The Blueprint would detail operational response at the Union and member state level to a large-scale cyber-attack using these well-established Crisis Management Mechanisms and the existing cybersecurity entities: CSIRTs Network, ENISA, European Cybercrime Centre at Europol, EU Intelligence Analysis Centre (INTCEN), EU Military Staff Intelligence Directorate (EUMS INT) and Situation Room (SITROOM) in INTCEN, EU Hybrid Fusion Cell and CERT-EU. In addition, the Scenario also requires that member states and EU Institutions establish an EU Cybersecurity Crisis Response Framework to make operational the Blueprint.

However, the overall architecture remains fragmented and incredibly complex. This is observable in Scenario I's current crisis response procedure. Under Scenario I, the procedure for crisis response begins with the Council, through the EU Integrated Political Crisis Response (IPCR) arrangements. Within the Commission, coordination will take place in accordance with the ARGUS rapid alert system (an IT platform enabling the Directorate General and services of the Commission to exchange relevant information in real time). If the

crisis encompasses an important external or CSDP dimension, the EEAS Crisis Response Mechanism (CRM) is activated. In addition to these mechanisms, the Blueprint would clarify the mandates of other actors under various conditions and circumstances. The number of actors and their complex mandates remains a central feature of the EU's Cyber Defence posture under Scenario I.

Lack of Resources

Third, the Cyber Security Package would increase resources, both to ENISA and through a potential Cybersecurity Emergency Response Fund to mitigate the effects of cyberattacks on member states. Such a fund would aid member states in their own crisis responses and provide a way for the EU to link EU institutions with member state responses.

However, resources under Scenario I remain highly distributed and diluted across a wide array and complex configuration of actors.

In sum, implementation of the Cyber Security Package, (Scenario I) would meaningfully increase operational cyber defence capabilities, while simultaneously maintaining the EU's largely advisory role. The overall structure/institutionalisation of defence capabilities remains largely consistent with the current state of play, with the Blueprint serving to further clarify crisis response at the EU level. Through the creation of an emergency response fund, Scenario I increases available resources and opens a potential avenue for additional EU–member state cooperation.

Given that we expect Scenario I, the Cyber Security Package, to be implemented soon with no more than minor revisions, the question then becomes:

- Does the 2017 Cyber Security Package go far enough?
- Does it adequately address the central limitations of the current EU approach to cyber defence?
- Does it significantly strengthen EU cyber defence capabilities?

This report concludes that although the Cyber Security Package makes important progress towards bolstering EU cyber defence capabilities, it does not adequately address the three central limitations present in the current approach. Given that this Base Case Scenario will likely be the state of play for cyber defence in the EU soon, the next section of this report focuses on how and to what degree Scenario II can build on and add to the progress achieved in Scenario I.

5.2.2 Scenario II – Establishing a Cyber Defence Coordinator

Building on the capabilities and institutional arrangements present in the Cyber Security Package, Scenario II seeks to provide oversight over and a coordination mechanism for the fragmented cyber defence architecture found in Scenario I. This is achieved through the creation of a cyber defence coordinator with the following responsibilities:

1. Monitoring of EU policy implementation throughout disparate EU and member state agencies and institutions.
2. Assessing the allocation of resources to institutions as necessary for the implementation of cyber defence strategies and operations.
3. Facilitating communication and coordination across EU and member state agencies and institutions.
4. Coordinating and consolidating cyber exercises. Today there are at least 10 cyber exercises happening almost every year in the EU, but in isolation (Cyber Coalition, Locked Shields, Cyber Europe, etc,). Consolidating and coordinating these through the Coordinator could achieve higher value with a lower chance of failure.
5. Coordinating information sharing at EU level. This function is much more consolidated today, but only happens in silos (e.g. the banking sector, the healthcare sector, the military community, etc.).
6. Creating an EU security operations centre with real capabilities and ambition. Today, Cert-EU has a very limited mandate and even more limited capabilities. Improving its role could bring immense value and enable cooperation at tech and political level,
7. Providing oversight over the entire EU defence architecture in order to maintain a cohesive EU readiness picture,
8. Providing policy advice based on the observed readiness picture, and
9. Serving as a single point of contact for EU institutions, member states and non-EU states.

The creation of a coordinator with these sets of tasks is neither unprecedented in cyber defence efforts outside the EU nor in other defence efforts within the EU.

Former White House Cybersecurity Coordinator[118] (colloquially known as the Cyber Tsar)	EU-Counter Terrorism Coordinator[119]
Created under President Obama to serve as a special assistant to the President in response to growing concerns over cybersecurity.	First appointed in 2007 by the EU High Representative to report to the Council in response to growing concerns over terrorism
Responsibilities included coordinating and integrating the various cyber policies within the US, ensuring the various agencies have the resources necessary for them to implement policies and carry out core functions, and monitoring and coordinating the US response to any major cyberattack.	Responsibilities include coordinating efforts undertaken by the Council, presenting policy recommendations, monitoring the implementation of existing strategy, and communicating with non-EU states.

As the European Political Strategy Centre notes in its 2017 report, such a cyber defence coordination position could mirror the configuration of the EU-Counter Terrorism Coordinator and report to the Council[120] or be embedded within a central cyber defence agency such as ENISA. Moreover, its tasks and responsibilities could similarly mirror those of the former White House Cybersecurity Coordinator, which was eliminated in May 2018.[121]

Given the limitations of Scenario I's approach to cyber defence, implementation of Scenario II would partially address a series of concerns around (i) the advisory role of the EU, (ii) the negative consequences of fragmentation, and (iii) the persistent lack of resources.

---

[118] In a heavily controversial decision, the cybersecurity coordinator position was eliminated in May 2018. For more information, refer to Perlroth, Nicole and David E. Sanger (2018), "White House Eliminates Cybersecurity Coordinator Role", *New York Times*, 15 May (https://www.nytimes.com/2018/05/15/technology/white-house-cybersecurity.html).

[119] For more information on the EU-Counter Terrorism Coordinator refer to the European Council's "Counter-Terrorism Coordinator" webpage: http://www.consilium.europa.eu/en/policies/fight-against-terrorism/counter-terrorism-coordinator/.

[120] European Political Strategy Centre (2017), "Building an Effective European Cyber Shield: Taking EU Cooperation to the Next Level", *EPSC Strategic Notes*, Issue 24, 8 May: p. 9 (http://ec.europa.eu/epsc/sites/epsc/files/strategic_note_issue_24.pdf).

[121] For more information, refer to Perlroth, Nicole and David E. Sanger (2018), "White House Eliminates Cybersecurity Coordinator Role", *New York Times*, 15 May (https://www.nytimes.com/2018/05/15/technology/white-house-cybersecurity.html).

Advisory Role

Pursuing Scenario II would not alter the character of the EU cyber defence capabilities found under Scenario I. Rather, it would improve the efficiency and efficacy of pursuing those goals. The EU would continue to support, contribute, assist, and promote, only now with greater horizontal (between EU institutions) and vertical coordination (between firms or national government and the EU).

The core activity of cyber defence, strategically and operationally, however, will continue to remain within the purview of member states.

Fragmentation

Mitigating fragmentation, identifying and addressing gaps in capabilities, and avoiding unnecessary duplication and overlap represent the greatest benefits in progressing from Scenario I into Scenario II.

Barriers are further reduced as the coordinator can and should function as a single point of contact for the EU's cyber defence posture. An answer to former US Secretary of State Henry Kissinger's question, "Who do I call if I want to call Europe?", would be to call first the EU Cyber Defence Coordinator who can then either address the concern directly or point the caller to the most relevant institution or person within the EU.

However, while the Cyber Defence Coordinator can mitigate some degree of fragmentation, their position continues to rest upon a complex, fragmented cyber defence ecosystem within the EU. The underlying institutional complexity will not disappear or be substantively replaced.

Lack of Resources

Given that the Cyber Defence Coordinator's responsibilities include overseeing the implementation of EU cyber defence strategies, initiatives, programmes, and/or policies, they are well suited to both assess and oversee EU allocation of resources to a wide array of institutions with some degree of responsibility for cyber defence.

Nevertheless, the approach presented in Scenario II will continue to be limited by the reality that resources will be highly distributed and diluted across a wide array and complex configuration of actors.

In sum, the creation of a cybersecurity coordinator position, whether embedded within ENISA or reporting to the Council, would address some of the persisting fragmentation concerns present in Scenario I. Scenario I's increase in capabilities and resources would now include an overarching layer of oversight and coordination. However, given that the coordinator would be assisting in the efficient and effective implementation of the existing advisory policy, the strategic and operational realities of cyber defence continue to remain primarily with the member states.

Similar to the conclusion of our discussion of Scenario I, the question then becomes:

- Does Scenario II go far enough?
- Does it adequately address the limitations present in the current EU approach and Scenario I?

This report concludes that Scenario II does not adequately address the full spectrum of limitations of concern. In particular, Scenario II lacks significant development of strategic and operational cyber defence capabilities at the EU level. Therefore, the next section of this report focuses on how and to what degree Scenario III will build on and add to the progress achieved in Scenarios I and II to further strengthen EU cyber defence capabilities.

7.1.1. Scenario III - Creating a Cyber Defence Agency

Building on the capabilities and institutional arrangements present in Scenarios I and II, Scenario III would centralise not only the coordination of the advisory policies previously discussed, but also create a Cyber Defence Agency that would be "equipped with adequate resources and executive competences to guarantee the speed, accuracy, efficiency and effectiveness" of EU cyber defence strategies and operations.[122] It is this executive competency and adequate resources that remain absent from both Scenarios I and II and yet, are an essential component of a strong EU cyber defence posture.

Importantly, this executive function would not preclude the role of member states in cyber defence. Instead, a Cyber Defence Agency would have a shared responsibility with EU member states to strengthen cyber defence analysis and capabilities. The EU's executive responsibility would exist only when necessary corrective measures based on the vulnerability assessment are not taken or in the event of disproportionate cyberattacks rendering the defence of a member state ineffective to such an extent that it risks putting in jeopardy the functioning of critical infrastructures elsewhere in the Union. As a result, member states would have the primary but not the sole responsibility for the management of their cyber defence.

This section is comprised of three main parts: a brief discussion of the organisation and governance for a Cyber Defence Agency, an analysis of the core competences/tasks of the agency, and an evaluation of the agency's ability to address persisting limitations to the current cyber defence approach, Scenario I, and Scenario II.

---

[122] European Political Strategy Centre (2017), "Building an Effective European Cyber Shield: Taking EU Cooperation to the Next Level", *EPSC Strategic Notes*, Issue 24, 8 May: p. 10 (http://ec.europa.eu/epsc/sites/epsc/files/strategic_note_issue_24.pdf).

Organisation and Governance:
What would an agency with 'executive competences' entail?

A Cyber Defence Agency would be an executive rather than an administrative or regulatory agency. As such, it would extend beyond ENISA, which is an administrative agency; however, for efficiency's sake, the foundation of the agency should be ENISA, given that it already exists, is undergoing reform, and overlaps in terms of the areas concerned with the proposed Cyber Defence Agency. In contrast to ENISA in its current formulation or in its Scenario I formulation, a Cyber Defence Agency would more closely resemble an agency residing under the Commission but steered inter-governmentally by a multi-stakeholder model. Since this agency will be deeply involved in many issues that have direct bearing on the national security concerns of member states, they will need to maintain a strong presence and share in governance.

The need for and creation of such executive competencies is not unprecedented. In fact, as Maastricht University's Professor Ellen Vos argues, due in part to the challenges increasingly facing the EU, "EU agencies are […] clearly 'on the move': they are increasingly proliferating and obtaining more and more discretionary powers".[123] In fact, in several instances, such as internal security and the financial independence of the ECB, EU agencies have historically been granted executive function and "put on par with the EU institutions in a variety of provisions in the Treaties".[124]

Furthermore, the utility of an agency with executive functions (although conceptually encompassed under the framework of a cyber coordination platform) was discussed and advocated for, as the European Political Strategy Centre notes in its 2017 report.[125] Significantly, this Task Force report has come to a similar recommendation.

Core Competencies

The Cyber Defence Agency should be built around "core activities" that could be carried out with greater efficacy and/or efficiency through centralisation.

Such a Cyber Defence Agency would be responsible for the coordination tasks outlined in Scenario II:

1. Monitoring of EU policy implementation throughout disparate EU and member state agencies and institutions.

---

[123] Vos, Ellen (2018), "EU agencies on the move: challenges ahead", *Swedish Institute for European Policy Studies*, p. 6.

[124] Ibid. p. 21.

[125] European Political Strategy Centre (2017), "Building an Effective European Cyber Shield: Taking EU Cooperation to the Next Level", *EPSC Strategic Notes*, Issue 24, 8 May: p. 10 (http://ec.europa.eu/epsc/sites/epsc/files/strategic_note_issue_24.pdf).

2. Assessing the allocation of resources to institutions as necessary for the implementation of cyber defence strategies and operations.
3. Facilitating communication and coordination across EU and member state agencies and institutions.
4. Coordinating and consolidating cyber exercises. Today there are at least 10 cyber exercises happening almost every year in the EU, but in isolation (Cyber Coalition, Locked Shields, Cyber Europe, etc,). Consolidating and coordinating these through the Coordinator could achieve higher value with a lower chance of failure.
5. Coordinating information sharing at EU level. This function is much more consolidated today, but only happens in silos (e.g. the banking sector, the healthcare sector, the military community, etc.).
6. Creating an EU security operations centre with real capabilities and ambition. Today, Cert-EU has a very limited mandate and even more limited capabilities. Improving its role could bring immense value and enable cooperation at tech and political level,
7. Providing oversight over the entire EU defence architecture in order to maintain a cohesive EU readiness picture,
8. Providing policy advice based on the observed readiness picture, and
9. Serving as a single point of contact for EU institutions, member states and non-EU states.

It would, however, also include the development of core operational capabilities needed for preventing or withstanding a cyber incident occurring in the EU. These additional responsibilities – core activities – include the development of EU:

10. Detection capabilities,
11. Technical attribution capabilities, and
12. Crisis response capabilities (including serving as a last resort for defence within the EU).

In order to strengthen **detection capabilities**, the Agency would have a dual mandate: to serve as a central repository for currently collected incident data and to generate shared threat intelligence and best practices for industry, domestic governments, and EU institutions/agencies.

These threat and vulnerability detection reports can take two forms. The first output focuses on awareness raising and best practices for critical and EU services and infrastructure. This effort would create a fuller operational picture of the current scope of vulnerability in the EU but also allow for the leveraging of these results directly into security and resilience measures and best practices/tangible next steps. The second output focuses on general awareness raising for the EU public. One potential format is a monthly EU Cyber Weather Report akin to those produced by the National Cyber Security Centre Finland

(NCSC-FI), which "sums up key incidents and phenomena in information security" in readily accessible formats for the general public.[126]

In order to bolster **technical attribution capabilities**, the Agency would utilise its detection capabilities in conjunction with private industry and EU cyber defence stakeholders to facilitate a joint-attribution forum. This forum would be limited to cyber forensics, but would serve as an important foundation for bolstering cyber security and resiliency efforts within the EU. Through this forum, the agency would be able to leverage a wider set of data and stakeholders than any single Government or National Cyber Agency could provide.

Moreover, the findings of this attribution forum could later be utilised for EU or member state political attribution for the purposes of deterrence by punishment and dissuasion through norms/taboos. Recall, punishment can occur outside of traditional military domains (e.g. sanctions or withdrawing diplomats), in the context of enforcing international laws, and in the process of championing norms (i.e. imposing reputational costs on violators).

In order to strengthen **joint crisis response capabilities**, the Agency would develop processes for tactical, operational, and strategic elements of EU cyber defence efforts in the event of a crisis. These processes would be evaluated and fine-tuned during periods of peace through exercises and trainings. While the Blueprint is an important first step, this process can and should become more streamlined. Cyber incidents are complex events; unduly complex or slow responses only increase the potential degree of disruption or destruction stemming from them.

In addition, the agency should build (with regulatory support) a new approach leveraging the compulsory disclosure and sharing requirements developed through the NIS Directive and the EU's General Data Protection Regulation (GDPR).[127] Information sharing should include not (only) pre-digested information coming from CSIRTs, but also the 5% of raw operational and intelligence data that is meaningful for governments and/or Operators of Essential Services (OESs) as they are termed in the NIS Directive. These collections of near real-time data should be analysed for intelligence purposes

---

[126] Cyber weather conditions oscillate between calm, worrying, and serious. The National Cyber Security Centre Finland (NCSC-FI)'s monthly Cyber Weather digest also includes information on denial-of-service attacks, malware and vulnerabilities, scams and phishing, spying, network performance, IoT, and trends in information security. For more information, refer to their website at https://www.viestintavirasto.fi/en/cybersecurity/informationsecuritynow/cyberweather.html.

[127] The impacts of the GDPR extend far beyond EU and privacy. In fact, the GDPR strengthens the civilian market by increasing security considerations as a function of privacy regulations. Moreover, this impact is felt in countries outside the EU. If a non-EU company has one EU national on the payroll, they are subject to GDPR.

and be used to develop wider, EU-based cyber situational awareness and serve as an important foundation for security and resilience strategies, operations, and tactics.

Moreover, while EDA will continue playing its role in cyber defence capability development, as the specific agency dedicated to EU Defence, the Cyber Defence Agency should serve as a last resort for defence against cyberattacks within the EU. Just as the EU serves as the last resort for member states facing major natural or manmade disasters by coordinating humanitarian aid from other member states, this agency should coordinate aid in the event of a cyber disaster. The agency should be able to intervene through Rapid Deployment Teams or Remote Teams in support of member states. This additional EU-based resilience capability will have to be built out over time through an iterative process of alignment, exercises, further alignment, and further exercises in order foster trust and increase effectiveness and efficiency. By pooling resources through this agency, potential EU targets have a far larger pantheon of resources at their disposal. Moreover, by serving as a last resort, the agency could bolster deterrence by illustrating to potential aggressors that no EU state or OESs need manage alone in this domain.

Addressing limitations with the current EU approach

With these three capacity building efforts, Scenario III most comprehensively addresses concerns around (i) the advisory role of the EU, (ii) the negative consequences of fragmentation, and (iii) the persistent lack of resources.

Advisory Role

Scenario III supplements the coordination efforts found in Scenario II with executive competences. As a result, a Cyber Defence Agency can both support member states in the implementation of their own strategies and operations, while simultaneously developing a core selection of strategic and operational capabilities itself.

However, some strategic and operational considerations should remain solely in the hands of states. The agency should not try to replace prerogatives from member states when dealing with priorities and responsibilities. For example, member states will continue to identify their own critical infrastructure and services (OESs) and allocate resources to improve security and/or resilience of critical infrastructure and services according to relevant and sovereign social and economic priorities, except when they fail to meet agreed upon basic levels of security/resilience or directly jeopardise shared infrastructures at the European level.

Fragmentation

Like the Coordinator, an agency will make it possible to mitigate fragmentation, identify and address gaps in capabilities, and avoid unnecessary duplication and overlap.

Barriers are further reduced in this Scenario, however, since an agency would function as a single point of contact for the EU's cyber defence posture. An agency can serve as a single point of contact for external actors (such as NATO or non-EU states) and internal actors (such as EU institutions, national governments, or industry).

An agency also provides additional benefits beyond what a Coordinator can provide, however, because an agency with executive functions allows for both a cohesive strategic vision for and oversight over cyber defence efforts and a cohesive or streamlined mechanism for real time crisis response in complex situations. As a result, an agency approach can lead to less institutionally complex and underspecified chains of command and communication in the event of crisis.

However, some degree of fragmentation in the cyber defence ecosystem will persist within the EU. Not all competencies will be moved up into the agency from other institutions or from member states. The underlying institutional complexity will not entirely disappear.

Lack of Resources

In terms of resource allocation, an agency can oversee funding allocation needed for the implementation of EU cyber defence strategies, initiatives, programmes, and/or policies. Allocation of funds should focus on identified priorities for achieving a basic level of resilience and security throughout EU institutions and member states. Funds could also be used to build shared systems or support research and industrialisation of specific technologies/solutions needed by the EU.

Notably, while a Coordinator could be overwhelmed, an agency is better equipped to allocate and monitor as well as make future recommendations for a budget of this scale and complexity. As such, one of the core contributions of an agency is to bolster EU cyber defence capacity through increased resource allocation and centralised budgetary oversight.

In sum, Scenario III extends the existing EU advisor capabilities found in Scenarios I and II while simultaneously adding a strategic and operational mandate at the EU level. Uniquely, an agency allows for the joint development of and cooperation towards EU detection, attribution, and incident response capabilities. The agency can also address resource allocation more effectively and efficiently.

In comparison to Scenarios I and II, the creation of an EU Cyber Defence Agency most substantively addresses both the limitations in the current EU approach and ecosystem as well strategic and operational considerations for developing a cyber defence posture more broadly. As such, Scenario III offers the greatest benefit when it comes to the goal of this Task Force: to strengthen EU cyber defence capabilities.

Moreover, it is worth noting that the importance of centralisation of management and strategic oversight have been echoed in other contexts. For example, in the US, a large country with a complex bureaucracy, the historical approach has similarly been piecemeal: "There have been numerous initiatives by federal, state and local governments, as well as by critical infrastructure operators themselves, to improve their respective cybersecurity postures, but these efforts have been hampered by a lack of coordination and resources."[128] To address this issue, retired General David Petraeus calls not for the US to "try harder" but for the creation of a "standalone agency", which would "be much more focused, capable and empowered than the current grab bag of governmental initiatives".[129] Similarly, for the EU, the issue is not the degree of effort but the current piecemeal approach.

5.3 Scenario Development and Assessment

Over the course of the Task Force meetings, we explored the dynamics of the threat space itself; potential defence strategies and specific cyber defence challenges; existing EU architecture and frameworks; and external frameworks developing within the US, Israel, and NATO as points of comparison. Emerging from these early discussions, each of the three scenarios was developed by the Chair, Coordinator, and Rapporteurs in conjunction with academic, industry, policy, and technical communities participating in this Task Force.[130]

In particular, the European Political Strategy Centre's 2017 report entitled, "Building an Effective European Cyber Shield: Taking EU Cooperation to the Next Level", served as an important foundation for Scenarios II and III. The seeds of these two scenarios can be found under the umbrella category of "Toward a European Cyber Coordination Platform".[131] They were separated

---

[128] David H. Petraeus (2018), "The Case for a National Cybersecurity Agency", The Belfer Center, 5 Sept. (https://www.belfercenter.org/publication/case-national-cybersecurity-agency).

[129] Ibid.

[130] Note: not all participants contributed to the development of the scenarios.

[131] European Political Strategy Centre (2017), "Building an Effective European Cyber Shield: Taking EU Cooperation to the Next Level", *EPSC Strategic Notes*, Issue 24, 8 May: p. 9 (http://ec.europa.eu/epsc/sites/epsc/files/strategic_note_issue_24.pdf).

and further developed and evaluated separately for the purposes of this Task Force.

Once formulated by the Task Force Chair, Coordinator, and Rapporteurs, these three scenarios were then formally presented and workshopped with the Task Force as a whole. Prior to the meeting, a written summary of each scenario was distributed to participants for their review. During the first half of the meeting, each scenario was briefly summarised, followed by a longer presentation by a separate participant who sought to advocate in favour of the scenario in question. For the second half, participants broke into three working groups, one per scenario, with a diversity of members ranging from industry to academia in each group. These multi-stakeholder working groups were comprised of 4-6 participants each.

In order to broaden the Task Force's appraisal of the comparative advantage of each scenario, each working group was tasked with discussing their scenario's value added or benefit to EU cyber defence efforts. This discussion was aided by a handout outlining a wide range of challenges facing defence efforts in cyberspace. In the handout, eleven broad categories were identified. Under each broad category, a series of specific tactical, operational, or strategic issues were highlighted. The eleven broad categories entailed 34 specific issues.

At the end of their working group discussion, and to provide a springboard for the larger group discussion, each individual participant was asked to rate their scenario's ability to address each of these 34 issues utilising a scale of 1-5 (very unlikely to very likely to address each issue).

For example, the following two issues for evaluation appeared under the second of eleven broad categories on the evaluation survey.

2). Cyber defense faces both a command and a communications challenge.

Therefore,

2A: does the scenario assist with and develop procedures for the communication of tasks and priorities laterally (i.e. at the operator level across technical teams, watch officers, etc.)?	**Very Unlikely** 1	2	3	4	**Very Likely** 5
2B: does the scenario assist with and develop procedures for the communication of tasks and priorities vertically (i.e. up and down the chain of command)?	**Very Unlikely** 1	2	3	4	**Very Likely** 5

Each individual completed this survey on the scenario assigned to their working group, although limited discussion occurred in each working group placing their own scenario into the broader context of the three potential

scenarios.[132] Participants did not complete a survey for the other two working groups, of which they were not a member.

The purpose of these surveys was to facilitate a more structured cross-scenario dialogue during the subsequent larger group discussion and to provide the Task Force with an additional metric of each working group's assessment of their own scenario. Notably, the tabulation of these surveys was not the sole means by which this Task Force determined its final recommendations. This determination was made based solely on the analysis of the comparative advantage of a Cyber Defence Agency over Scenarios I and II for bolstering EU cyber defence capabilities. This analysis, which was presented in the prior sections of this report, benefited from ongoing discussion between meetings and feedback, of which this informal survey was only one form.

Notably, the results of these surveys were consistent with the analysis presented in this report, namely that the perceived benefits of Scenario III to EU cyber defence far outstripped those of Scenario I and Scenario II. Scenario I's working group surveys received an average score of 81.2 out of a possible 170 points, Scenario II's working group surveys received an average score of 111 out of a possible 170 points, and Scenario III's working group surveys received an average score of 139.5 out of a possible 170 points. Importantly, these scores, as indicated above, represent an average score calculated from the individual surveys completed by members in each working group. As such, these figures represent a summary from each working group and not a unanimous opinion of all participants in the Task Force.

In conclusion, there was widespread agreement between the Task Force Chair, Coordinator, and Rapporteurs that Scenario III offered the greatest value added in general and in terms of addressing the 34 issues identified in the handout and, later, in the survey. This agreement was mirrored within the breakout working group discussions, the concluding plenary Task Force discussion following the breakout working group sessions, the Task Force's working group surveys, and subsequent feedback to distributed drafts of this report.

It is important to note, however, that agreement in the meetings and as demonstrated through each working group's survey results does not mean that support for Scenario III was unanimous. In fact, some participants did not view Scenario III as their preferred outcome.

---

[132] Note: participants only completed a survey for the scenario assigned and were unable to complete surveys for the remaining two scenarios. Each of these breakout sessions, however, contained discussion of and feedback for the other two scenarios. This feedback was incorporated into the final meetings, opened to broader discussion, and, at points, incorporated into this report.

PART IV
CONCLUSIONS AND RECOMMENDATIONS

6. CONCLUSIONS: THE CASE FOR A CYBER DEFENCE AGENCY

After determining in the previous sections of this report that the severity of the problem requires an increase in EU operational and strategic capacity, the question then becomes whether that increase in capacity would be best delivered through:

- a largely segmented, multilevel model (Base Case);
- a coordination mechanism (a cyber defence coordinator); or
- a new agency with executive functions (a Cyber Defence Agency).

This report concludes that increasing operational and strategic capacity through the creation of a Cyber Defence Agency provides the greatest cyber defence benefit to the EU. This Scenario addresses the existing limitations in the current EU approach as well as broader strategic and operational concerns. It also builds directly on the efforts currently being expended to implement the 2017 Cyber Security Package (Scenario I) and could easily leverage any efforts expended in the creation of a Coordinator (Scenario II).

6.1 Addressing the structural reality and technical trends of cyber defence

Notwithstanding the wide range of benefits previously discussed in this report, such as

- coordinating tasks across the EU,
- developing core operational capabilities needed for preventing or withstanding a cyber incident occurring in the EU, and
- addressing the central limitations of the current EU approach,

there are two central areas where a fully-fledged agency provides significant added value for bolstering EU cyber defence capabilities. An agency is well suited to the (i) structural reality of and (ii) technical trends within cyberspace and cyber defence. Each are worth emphasising here.

6.1.1 Structural Reality

We now live in an exponential world. In cyberspace, the terrain in need of defence is not a fixed or a relatively limited space. The IoT global market alone is expected to reach $8.9 trillion in 2020 as compared to $2.99 trillion in 2014.[133] In addition, malicious and non-malicious activity across these networks is rapidly evolving. The technological solutions we deploy become quickly outdated. As a result, a successful cyber defence model needs to be flexible and agile. An agency, in contrast to the current fragmented and highly distributed system resting on a network of institutions and initiatives each with their own mandates, governance models, budgets, and constituencies, is far more likely to be agile and/or flexible in practice.

6.1.2 Technical Trends

In addition, the growth of Artificial Intelligence (AI) as both an increasing concern for security and an important solution for security concerns presents unique challenges in the EU context. Specific purpose AI requires access to large amounts of data. As such, centralisation of data collection and cyber defence operations within an agency allows for quicker response times and threat assessment. A highly distributed and fragmented architecture, in contrast, will struggle to successfully leverage these tools.

6.2 Scenario II+: a first step

Given that the creation of a new agency might practically be a long-term process and the implementation of Scenario I is already underway, in the short-term, this report recommends that the EU commit to and embark on a path to an agency by first implementing a combination of Scenario II and Scenario III. This first step towards the creation of a Cyber Defence Agency has been termed Scenario II+.

Scenario II+ would entail:

1. the establishment of a cyber defence coordinator and
2. the creation of a technical attribution forum.

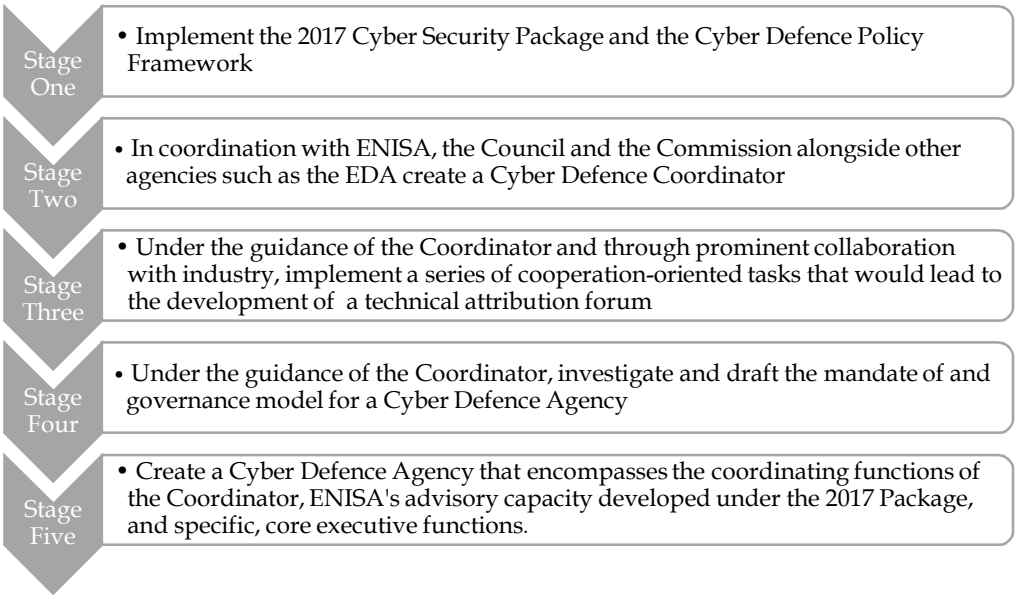
Given its design as a stepping stone, if the EU decides to embark on II+, it should be viewed as a commitment to transition towards an agency in the near future. Although II+ would not provide the same benefit to EU cyber defence capabilities that an agency would, it does address, in the short term, several core limitations of the current EU cyber defence architecture (fragmentation and lack

---

[133] Forbes (2017), "2017 Roundup of Internet of Things Forecasts", 10 December (https://www.forbes.com/consent/?toURL=https://www.forbes.com/sites/louiscolumbus/2017/12/10/2017-roundup-of-internet-of-things-forecasts/).

of resources) while at the same time targeting one of the core operational challenges of cyber defence strategies more broadly (attribution). Moreover, II+ could serve as a foundation upon which additional 'core functions' from Scenario III can be incrementally added on the way to a fully-fledged Cyber Defence Agency.

Five stages to the creation of an agency:



6.3 The continued importance of norms

Importantly, given the increasing militarisation of cyberspace and the impact it has on citizens, the EU should accompany these specific institutional efforts with a commitment to implementing cyber norms through declaratory principles or an eventual guiding legal framework.

As noted in this report, one central concern for the EU is the weaponisation of this domain for strategic purposes by state and non-state actors. Cyberspace is not merely a technical domain. It is a political domain in which we are witnessing a growing use of cyber weapons for political ends. This use has meant that states and non-state actors continue to actively develop and deploy cyber tools for political ends in isolation or in the context of hybrid operations or through the use of surrogates. Notably, civilians remain significant victims of these operations and efforts to apply norms (in the context of war but also outside of war) have so far fallen short.

Given that cyberspace is being used for strategic purposes, the EU cannot sit idly by and fail to develop its own cyber defence capabilities to protect its citizens, institutions, and member states. However, in developing these defensive capabilities, the EU must strike a balance between defending civilians and avoiding the further militarisation of cyberspace. Notably, the creation of a Cyber Defence Agency strikes this balance. The focus is on defending rather than weaponising.

Moreover, the creation of an agency does not, and should not, preclude a continued focus on norms. The lack of progress on implementing agreed upon cyber norms has enabled the continued militarisation of cyberspace. As a result, in an effort to protect civilians and to limit the use of cyberspace as a strategic domain, the EU should continue to support potential legal or normative frameworks but also, and more importantly, address the lack of consistent implementation of existing frameworks. Capitalising on its role in GDPR, Europe could play that of a 'norm superpower' and lead the effort in defining new norms to protect the civilian use of the internet and avoid its militarisation.[134]

The benefits of pursuing cyber norms alongside the creation of a Cyber Defence Agency are threefold. First, an agency does not preclude a norms-based defensive effort. The EU can, and should, seek to pursue strategies in order to prevent attacks as well as withstand attacks. While norms fall under the former category, much of the activity of the agency would fall under the latter. Second, creating an agency and pursuing norms are, in some instances, mutually supportive. For example, since the ability to enforce norms hinges in part on attribution, the establishment of a technical attribution forum is also a useful step towards this goal. Third, norms-based strategies offer an important defensive benefit to civilians globally. These normative efforts have the potential to set standards for behaviour and conduct in cyberspace that will simultaneously prevent attacks against the EU as well as extending protections to civilians outside the EU.

6.4 Now is the time to act

Cyber defence is critical to both the EU's prosperity and security.[135] Yet, the threat space it faces is vast in scope, highly interconnected, deeply complex, and rapidly evolving. In order for the EU to secure its own use of cyberspace, it must

---

[134] See Pupillo L. (2018), "EU Cybersecurity & the Paradox of Progress", CEPS Policy Insights, 2018/06 February 2018 (https://www.ceps.eu/system/files/PI2018_06_LP_ParadoxProgress.pdf).

[135] European Commission (2017), "Resilience, Deterrence and Defence: Building strong cybersecurity for the EU", Joint Communication to the European Parliament and the Council, 13 September (https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=JOIN:2017:0450:FIN).

be bold. The EU's current cyber defence capacity remains fragmented across and siloed within various institutions, agencies, and initiatives leaving the EU facing severe barriers in its pursuit of prevention and preparedness strategies and their corresponding operational requirements. The creation of a fully-fledged agency would be a critical step towards breaking down these silos and bringing all groups under its auspices to address the complex task of delivering on the promise of security for the Union in the cyber era. This is the right moment to act: "In the area of security, as in many other areas in Europe, fragmentation is what makes [the EU] vulnerable. Europe needs a genuine security union."[136] Cyber defence must most certainly form a central and robust component of that union.

[136] European Commission (2016) "President Juncker: Europe needs a genuine security union", Press Release AC/16/2142, 13 April (http://europa.eu/rapid/press-release_AC-16-2142_en.htm).

ANNEX I.
LIST OF TASK FORCE MEMBERS AND INVITED GUESTS AND SPEAKERS

Task Force Members

Chair:

Jaap de Hoop Scheffer, Leiden University and Secretary General of NATO from 2004-2009

Coordinator and rapporteur:

Lorenzo Pupillo, Associate Senior Research Fellow, CEPS

Rapporteurs:

Melissa K. Griffith, Ph.D. Candidate at the University of California, Berkeley

Steven Blockmans, Senior Research Fellow, CEPS

Andrea Renda, Senior Research Fellow, CEPS

Companies and European Organisations

Daniel Azrak, Manager Deloitte

Dan Cimpean, Partner, Cyber Risk Services towards the European Institutions, Deloitte

Lise Fuhr, Director General, European Telecommunications Network Operators

Harald Gruber, Head of Digital Infrastructure Division Projects Directorate, European Investment Bank

Stephane Mansat, Deputy Group CISO, Airbus

Giorgio Mosca, Director Strategies & Technologies, Security & IS Division, Leonardo Company

Liga Raita Rozentale, Director of EU Governmental Affairs for Cybersecurity Policy, Microsoft

Mark Smitham, EMEA Senior Cybersecurity Policy Manager, Microsoft

Jessica Zucker, EMEA Cybersecurity Strategist, Microsoft

European Institutions and Agencies

Filomena Chirico, Member of Cabinet of Vice President Jyrki Katainen, European Commission

Ana Hartmann, Political Administrator, Directorate General C- Foreign Affairs Enlargment & Civil Protection, Council of the EU

Iris Hiltunen, Stagiaire, Cabinet of Vice President Jyrki Katainen, European Commission

Tiia Lohela, Special Advisor, The European Centre of Excellence for Countering Hybrid Threats

Juha Mustonen, Director International Relations, The European Centre of Excellence for Countering Hybrid Threats

Vasileios Tsiamis, Policy Officer, Strategy and Policy, European Defence Agency

Representatives of the technical community:

Jean- Marc Rickli, Head, Global Risk and Resilience, Geneva Centre for Security Policy

Don Stikvoort, Chairman Open CSIRT Foundation

Representatives of European governments:

Turo Mattila, Deputy Representative, Political and Security Committee, Permanent Representation of Finland to the EU

Representative of intergovernmental organisation:

Antonio Missiroli, Assistant Secretary General, Emerging Security Challenges, NATO

Academia:

Christian Calliess, Professor for Public and European Law at Free University of Berlin, from 2015 till October 2019 Team Leader and Legal Adviser to the European Political Strategy Center (EPSC) advising the President of the European Commission

Stefano Fantin, Legal Researcher, Center for IT and IP Law, Katholieke Universiteit Leuven

John Peterson, Professor of International Politics, School of Social and Political Science, University of Edinburg

Invited Guests:

Margiris Abukevicius, Advisor, Defence & Cyber Issues, Permanent Representation of Lithuania to the EU

Jakub Boratynski, Head of Unit, Cybersecurity and Digital Privacy, DG Connect, European Commission

David Clark, Senior Research Scientist, MIT Computer Science and Artificial Intelligence Laboratory

Rami Efrati, Cyber Strategic Methods Expert, President of Firmitas Cyber Solutions

Christian Marc Liflander, Head of Section, Cyber Defence Division, NATO

Tarik Meziani, Council of the EU, Directorate General Foreign Affairs, Enlargement, Civil Protection

Tom Millar, Senior Advisor National Protection & Program Directorate, US Department of Homeland Security

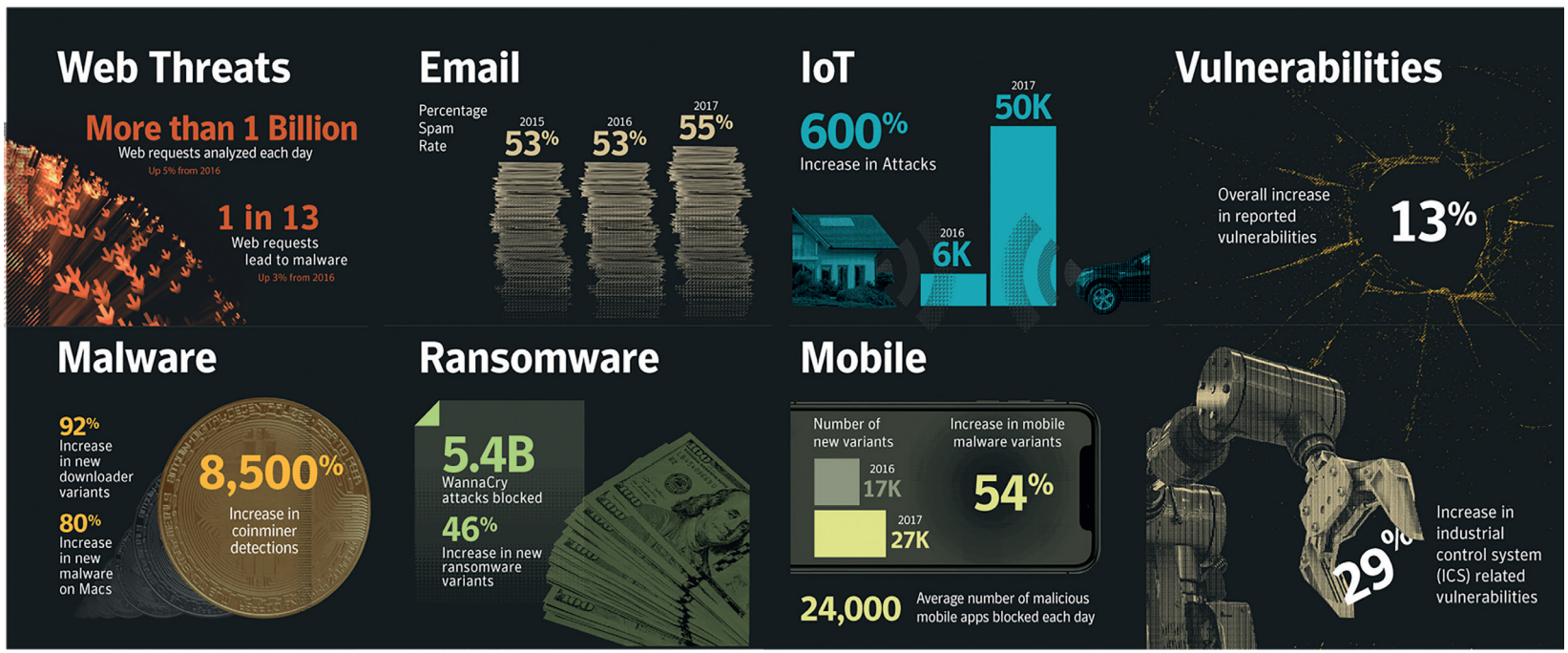
Giampiero Nanni, Government Affairs EMEA, Symantec

Christos Ntrigkogias, Major Hellenic National Defence General Staff, Cyber Defence Directorate

Spyridon Papageorgiou, Captain Hellenic National Defence General Staff, Cyber Defence Directorate

Patryk Pawlak, Brussels Executive Officer, EU Institute for Security Studies

Aidan Ryan, Head of Policy Unit, Department of Communications, ENISA



From Symantec's presentation to the CEPS Task Force on 23 March, 2018

This report puts forward the analysis and recommendations for the creation of an EU Cyber Defence Agency with executive competencies and therefore, the ability to develop and utilise strategic and operational capabilities at the EU level. Cyber defence is critical to both the EU's prosperity and security. Yet, the threat space it faces is vast in scope, highly interconnected, deeply complex, and rapidly evolving. In order for the EU to secure its own use of cyberspace, it must be bold. The EU's current cyber defence capacity remains fragmented across and siloed within various institutions, agencies, and initiatives leaving the EU facing severe barriers in its pursuit of prevention and preparedness strategies and their corresponding operational requirements. The creation of a fully-fledged agency would be a critical step towards breaking down these silos and bringing all groups under its auspices to address the complex task of delivering on the promise of security for the Union in the cyber era.

9 789461 387066

CEPS