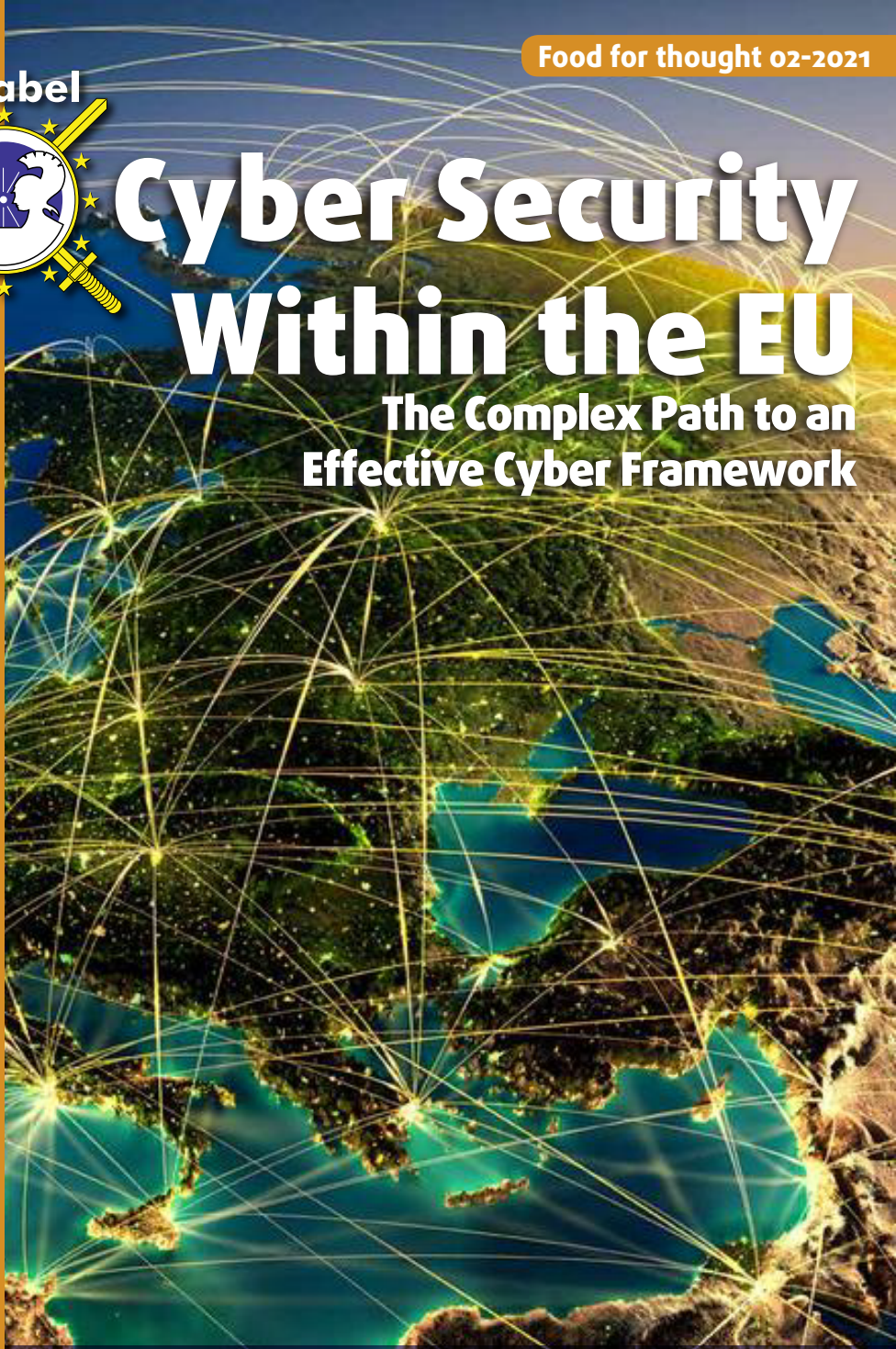
Finabel

Food for thought 02-2021

# Cyber Security Within the EU

## The Complex Path to an Effective Cyber Framework



AN EXPERTISE FORUM CONTRIBUTING TO EUROPEAN ARMIES INTEROPERABILITY SINCE 1953

FINABEL
European Army Interoperability Center

Written by
Christian Di Menna,
Candela Fernández Gil-Delgado,
Leandro Pereira Mendes, Milan Storms

This paper was drawn up by Christian Di Menna, Candela Fernández Gil-Delgado, Leandro Pereira Mendes, and Milan Storms under the supervision and guidance of Mr Mario Blokken, Director of the Permanent Secretariat.

This Food for Thought paper is a document that gives an initial reflection on the theme. The content is not reflecting the positions of the member states but consists of elements that can initiate and feed the discussions and analyses in the domain of the theme. All our studies are available on www.finabel.org

## TABLE OF CONTENTS

# LIST OF ACRONYMS

- 4C: Command, Control, Communications and Computers.
- AI: Artificial Intelligence.
- CBM: Confidence-Building Measures.
- CEO: Cyber Effect Operations.
- CERT: Indian Computer Emergency Response Team.
- CIDCC: Cyber and Information Coordination Centre.
- CII: Critical Information Infrastructure.
- CFSP: Common Foreign and Security Policy.
- CSBM: Confidence- and Security-Building Measures.
- CSCAP: Group of the Council for Security Cooperation in the Asia – Pacific.
- CSDP: Common Security and Defence Policy.
- CSR: Cyber Surveillance and Reconnaissance.
- DHS: Department of Homeland Security.
- DoD: Department of Defence.
- DoJ: Department of Justice.
- EDA: European Defence Agency
- EEAS: European External Action Service.
- ENISA: European Union Agency for Cybersecurity.
- EU: European Union.
- ICRC: International Committee of the Red Cross.
- ICT: Information and Communications Technology.
- IHL: International Humanitarian Law.
- NCIIPC: National Critical Information Infrastructure Protection Centre.
- NCSS: National Cyber Security Strategy.
- OCO: Offensive Cyber Operations.
- OSCE: Organisation for the Security and Cooperation in Europe.
- OPE: Operational Preparation of the Environment.
- PESCO: Permanent Structured Cooperation.
- PoC: Point of Communication.
- SOPs: Standard operating Procedures.
- SPP: Sector Specific Plan.
- TEU: Treaty on European Union.
- US/USA: United States of America.

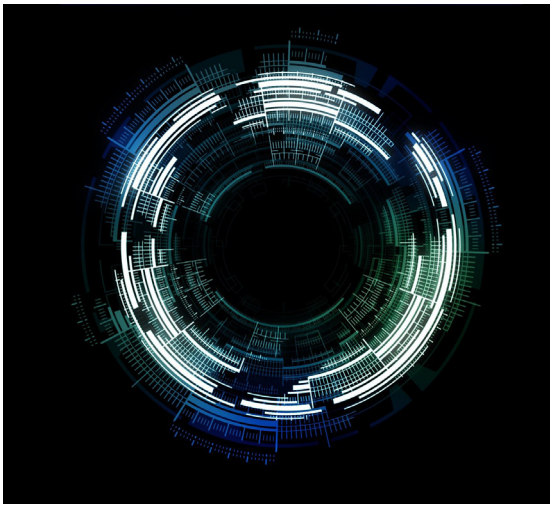
# INTRODUCTION

In this *Food For Thought*, we analyse the cybersecurity landscape within the European Union (EU). Cyberspace is challenging for the international community as it is part of our everyday lives. Yet, it remains relatively unregulated. The dearth of cyber specific regulations, and the diversity of players, makes the cyber domain the perfect environment for criminal activities. Thus, if the EU wants to continue to protect its citizens, an effective and comprehensive cyber framework is necessary. To this end, European institutions have been developing cyber capabilities, but despite this, there is still much work to be done.

First, Milan Storms analyses the EU policy framework on cyber operations and the possible development of international legal structures for offensive cyber operations. Then, Christian Di Menna examines the evolution of civil and military cyber policies in both India and the United States (US) in comparison with the EU. After this, Leandro Pereira Mendes discusses the challenges facing the EU regarding cyber policy and the development of cyber capabilities. Finally, Candela Fernández Gil-Delgado proposes an idea applicable to the cyber military domain: Confidence-Building Measures and offers possible solutions to EU challenges.

# A POSSIBLE FRAMEWORK FOR CYBERSECURITY

The European approach to creating a cyber defence framework has proven difficult in establishing an all-encompassing framework for cyber defence because of reasons of division of competences.[1] "Cyber Defence" is the term used by the EU to describe operations which are simultaneously within the realm of cybersecurity and defence. Only by creating a cyber defence framework, will the EU be able to build resilience to deal with cyber threats and to develop its own capabilities. As will be seen, the EU approach focuses on defensive cyber operations and can be described as *ad hoc.*



1. Article 5 of the Consolidated versions of the Treaty on European Union signed on the 7th of December 2012.

## EU Policy framework on cyber operations

Cyberspace is inherently transnational; therefore, it requires the same transnational approach to finding solutions. In Europe, such transnational approaches often lead to responses from the EU. Over time cyberspace has become the fifth domain of military operations (alongside land, sea, air, and space) and this complicates matters as defence and security are rarely an EU competence. Often member states retain exclusive competence in this field. Therefore, we will look at the European approach to cyberspace and cyber defence at the EU level, however, we will refer to the domestic level as needed. The EU, as an organisation with extremely deep interconnectedness between the member states, needs a common cyber defence framework more than any other international body because if one state is vulnerable to cyberattack, the whole Union becomes vulnerable.

In 2013 the European Commission acknowledged the importance of creating a policy framework on cybersecurity by creating the "Cyber Security Strategy for the European Union".[2] Following up on this, the European Council adopted The Cyber Defence Policy on 18 November2014.[3] This framework was updated in 2018, following a call by member states to do so.

The 2014 version had five objectives: 1) Support the development of member state cyber defence capabilities related to CSDP; 2) Enhance the protection of CSDP communication networks used by EU entities; 3) Promotion of civil-military cooperation and synergies with wider EU cyber policies, relevant EU institutions and agencies as well as with the private sector; 4) Improve training, education and exercises opportunities; and 5) Enhance cooperation with relevant international partners. These priorities show a recognition of the link between cybersecurity and defence[4].

When analysing EU documents on cyber defence, several attributes can be recognised. Firstly, it focuses on defensive rather than offensive cyber capabilities. This stresses the importance of measures that can protect member states, and the EU itself, from possible cyberattacks rather than using cyberattacks as a capability itself. When considering the legal framework for EU military cyber operations, attention needs to be paid to the domestic legal framework.

Secondly, as the EU is a supranational organisation adhering to the principle of conferral and the division of competences, there is a constant interplay between the state and the supranational levels.[5] This interplay with the state level is clearly visible in the policy framework. Therefore, the first pillar of a European defence policy regarding cyberspace is the state or domestic pillar, strengthening the member states' policies and supporting the developments of the member states' capabilities.[6] At present, almost every member state of the EU has a national cybersecurity strategy or has incorporated cybersecurity into their national strategies. At the state level, we can see that certain states are developing both cyber-defence and cyber-offensive capabilities.[7]

2. Joint communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of regions on Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace of 7 February 2013, JOIN (2013) 1 final.
3. EU Cyber Defence Policy Framework adopted 18 November 2014, nr. 15585/14.
4. European Defence Agency, "Summary on cyber defence",. Available at: https://www.eda.europa.eu/what-we-do/activities/activities-search/cyber-defence
5. The principle of conferral, laid down in article 5 TEU, encompasses that the EU only has those competences that are granted to it by the member states. If that is not the case that competence shall stay with the member states itself.
6. EU Cyber Defence Policy Framework (2018 update) adopted on 19 November 2018, nr. 14413/18.
7. Quoted in Mike Levine, "Russia Tops List of 100 Countries that Could Launch Cyberattacks on US," ABC News May 18, 2017. Available at: https://abcnews.go.com/US/russia-tops-list%20-100-countries-launch-cyberattacks-us/story?id=47487188

Because Common Security and Defence Policy (CSDP) missions largely depend on the capabilities of the member states, the first task of the EU framework is to ensure that there are no vulnerabilities in these domestic structures that could possibly be exploited. EU military operations, most often CSDP missions, rely on the Command, Control, Communications and Computers (4C) infrastructure of member states. Understanding this, it becomes clear that cyber defence and operations within the EU require convergence.

As defence largely remains a competence of the member states, the EU aims to support them in various ways. One example is the training and education platform launched to support cyber defence training and common cyber defence exercises.[8] Other examples include sharing and pooling projects for military operations aimed at harmonising national legislation and practices.

The third characteristic of EU cyber defence is the patchwork nature of the framework. The fields of Common Foreign and Security Policy (CFSP) and CSDP have witnessed a long period of inactivity due to a lack of participation from the member states. Therefore, the focus has been on guiding cooperation between member states and the organs of the EU. However, recent projects have addressed this somewhat.[9] As such, EU foreign, security and defence policy has witnessed a revival. Conventional CSDP missions are being deployed to provide practical security assistance, and use has been made of the articles on Permanent Structured Cooperation (PESCO)[10].

These new impulses have had a positive influence on cooperation in cyber operations. The best example is the emergence of eight cyber-related PESCO projects.[11] One of the most prominent is the "cyber rapid response teams and mutual assistance in cybersecurity". Six EU countries have signed a declaration of intent for the development of this project on the 25th of June 2018. The European External Action Service (EEAS) welcomed the initiative in paving a way towards common cyber defence. This shows that PESCO is more than just an instrument within the cyber defence framework. It could develop itself as a great driving force within the field of cyber defence. These teams consist of cybersecurity specialists who can react, neutralise, and investigate cyber incidents. For the EU, this represents a capacity to respond.[12] As has been stressed, these efforts are focused on defensive cyber operations.

Other projects such as "Cyber Threats and Incident Response Information Sharing Platform" may point the way forward for cyber defence, as member states remain reluctant to relinquish their powers in the field of defence and security, PESCO offers a solution as participation is voluntary. Currently, however, most projects have attracted a small number of participating countries. The Cyber and Information Coordination Centre (CIDCC) project for example, consists of only three member states (Germany, Hungary, and the Netherlands)[13].

The next cog in the cybersecurity and cyber defence machinery of the EU are the solidarity and the mutual assistance clauses.[14] These clauses were introduced with the entry into force of the Treaty of Lisbon (2009). Ultimately they were introduced to create an

8. EU Cyber Defence Policy Framework adopted November 18, 2014, nr. 15585/14.
9. Andrew Huckle, "The Evolution of the European Union's Common Security and Defence Policy", E-International relations. Available at: https://www.e-ir.info/2016/07/07/the-evolution-of-the-european-unions-common-security-and-defence-policy
10. For a full list of CSDP missions see: https://eeas.europa.eu/headquarters/headquarters-homepage/430/military-and-civilian-missions-and-operations_en
11. For a full list of cyber related PESCO projects see: https://eucyberdirect.eu/content_knowledge_hu/cyber-related-pesco-projects/
12. Information and list of participating countries see: https://pesco.europa.eu/project/cyber-rapid-response-teams-and-mutual-assistance-in-cyber-security/
13. Information and list of participating countries see: https://pesco.europa.eu/project/cyber-and-information-domain-coordination-center-cidcc/
14. Article 42(7) of the Consolidated versions of the Treaty on European Union signed on the 7th of December 2012.

concept of cooperation and joint action. If a member state of the European Union were to suffer from a crisis (solidarity) or be the target of armed aggression (mutual assistance), all member states are expected to aid and act jointly to help the affected state. Due to the interconnectedness of member states and the risks from cybersecurity, it has been debated whether the clauses could be invoked.

The question therefore is; if a member state fell victim to a cyber-attack, would this require other member states to assist the targeted state? This may be problematic because of the vagueness that surrounds the mutual assistance clause. A concrete policy framework regarding mutual assistance is lacking. This is in contrast with the solidarity clause: the council adopted a decision on the implementation of this clause in 2014.[15] However, this does not mean the mutual assistance clause is totally redundant. In 2015 France invoked the clause (art 42 (7) Treaty of the European Union - TEU) for the first time as a response to the Paris terrorist attacks of 13 November 2015.[16] However, due to a lack of an implementation decision, this clause may be too vague to play an effective role in countering attacks and more specifically for this study on cyber-attacks.

When discussing the legal framework of cyber operations, a distinction can be made between offensive and defensive cyber operations. At present PESCO and the clauses of Article 42 have revolved around cyber defence and protection against attack. We must ask then: is there a legal framework for offensive cyber operations? Can such actions be planned under international law as it now stands? We will address these questions below.

## Offensive cyber operations and international humanitarian law

Offensive cyber operations are defined as "computer activities to disrupt, deny, degrade, and/or destroy".[17] These have proven difficult to correctly attribute thus, demonstrating a need for a clear legal framework regarding offensive cyber operations as such a framework, may prove to be a solution to the attribution problem.[18]

As society evolves and interconnectedness and networking is becoming increasingly important and since cyberspace is of major importance to every aspect of modern society, there are strategic advantages to be obtained from targeting the networks of competitor states or actors. Offensive cyber operations may have several purposes: 1) exploiting information on a secured network; 2) destroying data on a certain network or certain systems; 3) altering data to show confusion; and 4) denying service to a network.[19] As states and their militaries become more reliant on networked technology, targeting these networks could be disastrous and therefore, providing strategic advantage for the attacker. Although there are relatively few states who publicly acknowledge an offensive cyber policy, the operations of certain states indicate that they are using cyber capabilities for military objectives.[20]

One of the reasons a legal framework for military cyber operations may prove difficult to construct is the relationship between the

15. Council decision of 24 June 2014 on the arrangements for the implementation by the Union of the solidarity clause, OJ L 192, 1.7.2014, p. 53–58.
16. European Council Briefing EPRS, "Activation of Article 42(7) TEU France's request for assistance and Member States' responses". Available at: https://www.europarl.europa.eu/RegData/etudes/BRIE/2016/581408/EPRS_BRI(2016)581408_EN.pdf
17. Max Smeets, "The Strategic Promise of Offensive Cyber Operations", Strategic Studies Quarterly, 2018, Vol. 12, No. 3, pp. 90-113.
18. See *Food For Thought:* "Understanding Cybercrime: Current Threats and Responses", on the challenges of cybersecurity and more importantly the chapter on responsibility written by L. Mendes. Available at: https://finabel.org/understanding-cybercrime-current-threats-and-responses/
19. Herbert S. Lin, "Offensive cyber operations and the use of force. Available at: https://jnslp.com/wp-content/uploads/2010/08/06_Lin.pdf
20. Tom Uren, Bart Hogeveen, and Fergus Hanson, "Defining offensive cyber capabilities", Australian strategic policy institute. Available at: https://www.aspi.org.au/report/defining-offensive-cyber-capabilities.

military and cybersecurity. Brecher suggests this causes an uneasy relationship between the rules governing military action and offensive cyber operations[21]. This is because cyber operations do not resemble traditional military actions at all, and, the current legal regime was created for traditional military, not cyber operations. However, offensive cyber operations like shutting down critical infrastructure via the internet, may have the same consequences as kinetic attacks. Due to the maturing of cyber technology, the present international legal framework no longer reflects the reality of warfare and use of force as experienced today. This raises the question: can we apply international humanitarian law (IHL) to offensive cyber operations? The answer is yes. However, the challenges of cybersecurity may make it difficult. This is because an action must qualify as an 'armed attack' for international humanitarian law to apply. Brecher notes that one could try an effects-based test to determine whether an offensive cyber operation would result in an 'armed attack'.[22] That test may prove to be difficult in reality and the consequences of such may be severe. If one is unable to determine whether an 'attack' was an 'armed attack', their response may constitute a prohibited use of force as described by article 2(4) of the United Nations Charter.[23]

Another consideration in the relationship between cyber operations and IHL is whether the application of IHL legitimises the militarisation of cyberwarfare or the use of cyber warfare as an instrument. The International Committee of the Red Cross (ICRC) is straightforward in its position. It states that "affirming the applicability of international humanitarian law does not legitimise cyber warfare, just as it does not legitimise any other form of warfare".[24] Restricting cyber operations during armed conflict does not legitimise the use of hostile cyber operations, nor render their use lawful. As cyber operations have become a method of warfare, the ICRC is of the opinion that international humanitarian law can pose limits on the use of cyber operations rather than being an all-encompassing framework for cyber operations. The usefulness of IHL lies in the fact that it can restrict the consequences of cyber operations and a limitation in its application to cyber operations that apply to armed conflicts.

A cyber operation alone will rarely be enough to qualify as an armed conflict. A test to determine what legally constitutes armed conflict was drawn up in the Tadic case, which noted that "any resort to armed force between states will result in an armed conflict (or non-state actors, which will result in a non-international armed conflict)".[25] It is difficult to establish at what point, a state or a non-state actor, resorts to armed force when dealing with kinetic action. It is even more tricky to distinguish the tipping point for cyber operations.

A cyberattack, or an offensive cyber operation, itself, has never been qualified as an 'armed attack'. Therefore, the only way IHL will apply to offensive cyber operations will be if an armed conflict is underway. Even then, the rules are written with kinetic attacks in mind, further stressing the importance of a framework for offensive cyberattacks. A legal framework could restrict the negative consequences of such attacks whilst IHL tries to do this it does not seem fit to consider the special nature of cyberattacks.

21. Aaron P. Brecher, "Cyberattacks and the covert action statute: towards a domestic legal framework for offensive cyberoperations", 2012, Michigan Law Review, vol. 111.
22. Ibid.
23. United Nations, Charter of the United Nations, October 24, 1945, 1 UNTS XVI. Available at: https://www.refworld.org/docid/3ae6b3930.html
24. Helen Durham, "Cyber operations during armed conflict: 7 essential law and policy questions". Available at: https://blogs.icrc.org/law-and-policy/2020/03/26/cyber-armed-conflict-7-law-policy-questions/.
25. ICTY 15 July 1999, Prosecutor v. Dusko Tadić, IT-94-1-AR72.

# INDIA AND USA CYBER POLICIES IN RELATION TO THE EU

This chapter focuses on cyber policy in India, and the US, in relation to the EU. First, through India's cyber policy and its cyber agency. Then, through the US' cyber military tool "Beyond the build" and focusing on the 2018 National Cyber Strategy. Finally, we highlight the characteristics of the cyber-military domain and cyber-military operations in comparison with the EU.

## India's Cyber Policy

Early cybersecurity in India was limited due to the lack of technology and participation in international voluntary export regimes such as the Wassenaar Arrangement.[26] However, India has related its cybersecurity to national security from a state-centric, instead of socio-economic, perspective.[27]

In 2000, India enacted its first Information Technology (IT) law; the "Information Technology Act (IT Act)". This act was not adequate in dealing with cyberspace as India's national network was still at an embryonic stage. For the first time, the IT Act penalised the practice of hacking.[28] However, it contained rudimentary clauses for data protection, and there were no rules pertaining to cybersecurity. The main objective of this act was to protect the business interests of the IT-enabled services industry.[29] As such, there was a clear failure to understand the real near-term impact of the internet, which would see the number of cyber-attacks increase in the coming years. This undoubtedly had an impact on the Cybersecurity Policy.

In 2008, the IT Act was amended, and a new agency called National Critical Information Infrastructure Protection Centre (NCIIPC) was created. Entering into force in 2014, the NCIIPC was charged with protecting designated Critical Information Infrastructure (CII) and with establishing the Indian Computer Emergency Response Team (CERT-In) to respond to cyber incidents in non-critical sectors.[30] The functions of the agency include protection of cyberspace, identification of threats to cybersecurity and security risks caused by inadvertent software.[31] [32] A lack of guidelines or Standard operating Procedures (SOPs) for the event of a cyberattack, has meant that sectors without a Sector Specific Plan (SPP) designed to ensure harmony between government and industry, remain vul-

26. Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies.
27. Divij Joshi, "A comparison of legal and regulatory approaches to cyber security in India and the United Kingdom", November 12, 2017. The Center for Internet & Society.
28. Ibid.
29. Saikat Datta, "Cybersecurity, Internet Governance and India's Foreign Policy: Historical Antecedents, Internet Democracy Project", 2016.
30. Saikat Datta, "Cybersecurity, Internet Governance and India's Foreign Policy: Historical Antecedents, Internet Democracy Project", 2016.
31. Divij Joshi, "A comparison of legal and regulatory approaches to cyber security in India and the United Kingdom", November 12, 2017. The Center for Internet & Society.
32. Point 2, Guidelines for the Protection of National Critical Information Infrastructure "take all necessary measures to facilitate protection of Critical Information Infrastructure, from unauthorized access, modification, use, disclosure, disruption, incapacitation or destruction, through coherent coordination, synergy and raising information security awareness among all stakeholders." Available at: https://nciipc.gov.in/documents/NCIIPC_Guidelines_V2.pdf


nerable.[33]

In 2013, the National Cyber Security Policy was established following several cyberattacks. It outlines the characteristics of cyberspace. It utilises extensive methods to ensure cybersecurity through identification of threats; through information sharing between parties; as well as investigation and coordinated responses.[34] It underscores the importance of data protection, and protection against cybercrime from a socio-economic perspective. However, it has so far failed to create concrete cybersecurity measures.

Recently, Indian cybersecurity policy has focused on risk factors in the cyber domain, and it seeks to tackle threats to national security, focusing more on cyber defensive strategies, than on cyber offensive capabilities.[35]

Compared to India, the EU considers the cyber domain to be part of several internal policy areas: justice, home affairs, digital single market, and research. In external policy, cybersecurity forms part of the emerging defence policy. In comparison to India, EU policy in the cyber field resulted in the "2013 Cybersecurity Strategy" supported by three additional EU strategies: 1) the European Agenda on Security, linked to cybercrime as it is aimed at law enforcement and judicial response; 2) the Digital Single Market Strategy, whose objective is the creation of better access and conditions for the digital economy; and 3) the Global Strategy, which aims to create a stronger role in the world through a new commitment and approach to cybersecurity.[36] Overall, the EU aims to create a safe cyber environment for its fundamental rights and values. There are five objectives essential to achieving this: 1) increase cyber resilience; 2) reduce cybercrime; 3) develop cyber defence policies and capabilities; 4) develop industrial and technological cybersecurity resources; and 5) establish an international cyberspace policy aligned with EU values.[37]

33. Ibid.
34. Ibid.
35. Ibid 31.
36. Point 2, Guidelines for the Protection of National Critical Information Infrastructure "take all necessary measures to facilitate protection of Critical Information Infrastructure, from unauthorized access, modification, use, disclosure, disruption, incapacitation or destruction, through coherent coordination, synergy and raising information security awareness among all stakeholders." Available at: https://nciipc.gov.in/documents/NCIIPC_Guidelines_V2.pdf
37. Challenges to effective EU Cybersecurity policy, European Court of Auditors, 2019.

## Indian Defence Cyber Agency

In 2019, the Indian Government founded the Indian Defence Cyber Agency, this is a tri-Agency formed by Army, Navy and Air Force personnel. As it is governed by the Defence Intelligence Agency, which is controlled by the Ministry of Defence, it focuses on the military cyber domain: particularly the international offensive, and defensive, cyber capabilities of the state.[38] It was created to combat international cyberattacks on military targets. Yet, one of the main issues facing this agency is the lack of solid national legislation: no policy documents, governmental or parliamentary acts exist to explain in detail the domain of competence, or, what constitutes "military cybersecurity".

Another issue faced by the agency is recruitment: Personnel need to be highly qualified and finding people with deep knowledge of the cyber domain is difficult due to a lack of knowledge and private-sector competition. However, the creation of the Defence Cyber Agency is an important step for India to become more secure in the cyber domain.

Regarding the EU, the European Union Agency for Cybersecurity (ENISA) and the European Defence Agency (EDA) both created in 2004, are tasked with combating t cybersecurity threats within the civil and military domain.

ENISA is dedicated to achieving a high level of common cybersecurity across Europe. As with India, the agency has released an EU Cybersecurity Act, thus contributing to EU cyber policy. It has enhanced the trustworthiness of ICT products, services, and processes with cybersecurity certification schemes. It cooperates with member states and EU bodies and helps Europe prepare for future cyber challenges.

EDA helps to improve the defence capabilities of the different member states through European cooperation. It has become the 'hub' for European defence cooperation, especially in areas such as military mobility and cyber threats. Furthermore, the EDA has a supporting role vis-à-vis their advisory board regarding the project's dual-use or military cybersecurity potential. It makes sense to involve EDA in technological innovation that is beneficial to Europe's militaries and the reliance of Europe's militaries on cutting-edge cyber technologies.[39] [40]

## US Cyber Military Policy

In the US, military strategy is built on a foundation of information dominance. The US has invested heavily in transforming its cyber forces. Leading the way is "Beyond the Build" the 2015 cyber strategy issued by the Pentagon. It discusses the necessity of "Cyber Effect Operations" (CEO) to impair, not only the machines but also the data contained therein[41]. This applies to all spheres of national activity affecting war, diplomacy and law enforcement[42]. Additionally, there is a deeper dimension to CEO regarding "Information Operations" which highlights how information can impact military power through cyber means. The Joint Chiefs of Staff have identified how information can be used in an integrated manner during military operations as a sub-component of an information warfare strategy[43]. "Beyond the Build" recognises the weakness of the Department of Defence

38. Nidhi Singh, "India's New Defence Cyber Agency", 2019. Available at: https://www.medianama.com/2019/05/223-indias-new-defence-cyber-agency-nidhi-singh-ccg-nlud/
39. European Defense Agency, "European Defence Matters". Available at https://www.eda.europa.eu/webzine/issue18/focus/eda-s-growing-role-in-cybersecurity
40. European Defence Agency policies. Available at https://www.eda.europa.eu/what-we-do/our-current-priorities/eu-policies
41. Cherian, Munish, "Securing Cyberspace: International and Asian Perspectives", 2016, Pentagon Press.
42. United States, The White House, "Presidential Policy Directive 20: U.S. Cyber Operations Policy", 2012. Available at: http://fas.org/irp/offdocs/ppd/ppd-20.pdf
43. US JCS. Cyberspace Operations, No. 9.

(DoD) in operating with a lack of cyber awareness. The 2015 Strategy stresses that to be effective in cyber warfare, a country needs to plan, structure, and train its forces.

The 2015 Strategy is based on four pillars which include: 1)the importance of giving commanders "cyber tools in all phases of operations" and increasing capacity and capability to combat cybercrime; [44] 2) R&D innovation: the need to face cybersecurity through rapid technological innovation, to develop an exceptional cyber workforce based on a relationship between talented civilian, and military personnel"; 3) military education of officers in the cyber policy field; 4) war avoidance and peacebuilding through diplomacy.

In 2018, a new National Cyber Strategy was developed with four pillars: 1) defence of the homeland by the Department of Homeland Security (DHS) through protection of networks, data, and access to agency information systems, for cybersecurity purposes; 2) promotion of American prosperity by nurturing a secure, digital economy and fostering strong domestic innovation, and strategies with the collaboration of both private sector and civil society; 3) preservation of peace and security through strengthening the United States' deterrence and development, if necessary, of tailored strategies to ensure adversaries understand the consequences of their cyber behaviour;[45] 4) expansion of American influence abroad to extend cyber capacity building.[46]

Regarding the US cyber military domain, the Department of Defense (DoD) is the main actor: its mission is to secure cyberspace and help to mitigate the risks to national security. It can set specific missions for this purpose. [47] [48]

US cyber operations are divided into four categories: 1) shaping cognition by use of information to influence populations; 2) Cyber Surveillance and Reconnaissance (CSR) through which e-companies, states and other entities gather data; 3) Operational Preparation of the Environment (OPE) which plans to take advantage of computer systems; 4) Cyberspace attacks through Offensive Cyber Operations (OCO). [49] [50]

Concerning the EU, almost all member states have their own National Cyber Security Strategy (NCSS). These serve as a key policy feature, helping to tackle risks which have the potential to undermine the achievement of economic and social benefits reaped from cyberspace. These include a military perspective of cyber-defence in their national approaches".

## US Cyber Policy Updates

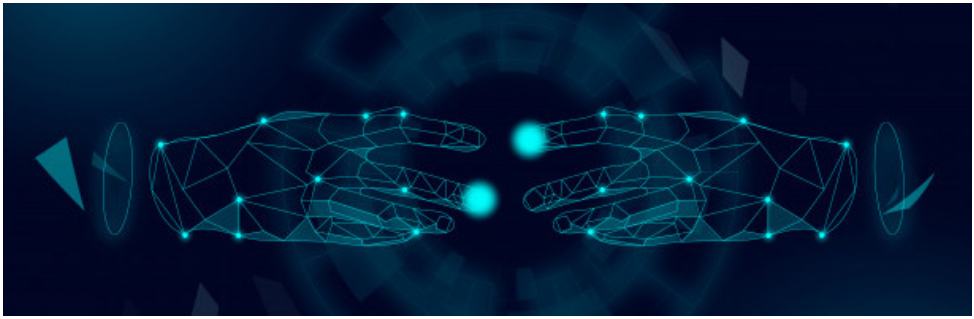
The US government's Cyberspace Solarium Commission[51] published a report on cyber activity. The report is divided into six pillars: [52] 1) Reform the U.S. Government's Structure and Organisation for Cyberspace. This includes an overhaul of the National Cyber Strategy based on an approach of cyber deterrence, resilience, and public-private collaboration; 2) Strengthen norms and non-military tools. The commission recommends the creation of an Assistant Secretary of State for

44. US Cyber Command, No 21
45. Ibid.
46. National Cyber Strategy, US, 2018
47. G. Alexander Crowther and Shaheen Ghori, "Detangling the Web: A Screenshot of U.S. Government Cyber Activity," 2015, Joint Force Quarterly, Issue 78, pp. 75–83. Available at: http://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-78/jfq-78.pdf
48. Crowther, "National Defense and the Cyber Domain", The Heritage Foundation, 2018.
49. Crowther, "National Defense and the Cyber Domain", The Heritage Foundation, 2018.
50. Ibid.
51. The Commission is a bicameral, bipartisan, intergovernmental body created by the 2019 National Defence Authorisation Act and charged with developing and articulating a comprehensive strategic approach to defending the United States in cyberspace
52. Robert Chesney, "The Cyberspace Solarium Commission Report: A Lawfare Series", March 11, 2020, . Available at: https://www.lawfareblog.com/cyberspace-solarium-commission-report-lawfare-series

cyberspace, and engagement in setting international IT standards and law enforcement activities; 3) promotion of national resilience by implementing capacity for post-attack recovery, the codification of sector-specific risks, codifying the cyber response and promoting of public awareness through digital literacy and civic education; 4) reshaping the cyber ecosystem toward security with regards to creating a national data security and privacy protection law; 5) operationalise cybersecurity collaboration with the private sector, through the creation of a public-private integrated cyber centre to analyse the national cyberspace; and 6) preserve and employ the military instrument of power and all other options to deter cyberattacks. The main proposition is to develop a force-structure for the Cyber Mission Force to ensure appropriate structure and capabilities.[53]

While US cyber policy seems complete, authors like Di Pane identified two notable gaps. First, in case of major cyberattack, it may endanger the economy, infrastructure and national defence. Second, deterrence must be approached with both offensive and defensive capabilities.[54] Furthermore, Kennedy adds that the report's focus on vulnerability management does not work, because it should offer comprehensive guidance on how to achieve an improved "combined arms" defence in depth.[55]

As mentioned previously, the EU Cyber Defence Policy Framework seeks the protection of the EU Common Security and Defence Policy communication and information network. PESCO, and cooperation with NATO form part of EU cyber defence. Moreover, the Joint Framework on countering hybrid threats aims to highlight how cyberattacks could be carried out as disinformation campaigns on social media. The strategy aims to ensure an open, global internet, with strong safeguards and protection for fundamental rights. There are three instruments necessary for achieving these objectives: regulatory, investment, and policy initiatives. These impact three main areas: resilience, technological sovereignty; the operational capacity to prevent, deter and respond; the cooperation to advance a global and open cyberspace.



53. Cyberspace Solarium Commission Executive Summary, US, 2020.
54. James Di Panne, Cybersecurity: Five "Keepers" in the Cyberspace Solarium Commission Report, August 20, 2020. Available at: https://www.heritage.org/cybersecurity/report/cybersecurity-five-keepers-the-cyberspace-solarium-commission-report
55 Chris Kennedy, "Three Major Gaps in the Cyberspace Solarium Commission's Report that need to be addressed", 2020 . Available at: https://www.helpnetsecurity.com/2020/07/09/cyberspace-solarium-commissions-report/

| India | US | EU |
|---|---|---|
| **Cyber Policy** | | |
| **2000 IT Act and creation of the NCIIPC (2008).**<br>Identify threats to cybersecurity.<br><br>**2013 Policy:** Ensure cybersecurity<br>1) Identification of threats,<br>2) Information sharing between parties, investigation and coordinated response.<br>3) Data protection and protection of the infrastructure. | **2015 Pentagon Cyber Strategy "Beyond the Build".**<br>1) Give Commander's cyber tools.<br>2) R&D Innovation<br>3) Military Education<br>4) War avoidance and peacebuilding<br><br>**2018 New National Cyber Strategy**<br>1) Defend the DHS.<br>2) Promote American prosperity fostering strong domestic innovation.<br>3) Preserve peace and security by strengthening the US ability to deter and punish those who use cyber tools for malicious purposes.<br>4) Expand American influence abroad | **2013 EU Cybersecurity Strategy**<br>1) Increase cyber resilience.<br>2) Reduce cybercrime.<br>3) Develop cyber defence policies and capabilities.<br>4) Develop cybersecurity resources.<br>5) Establish an international cyberspace policy within the EU values.<br><br>**2020 EU Cybersecurity Strategy**<br>1) Contribute to a cyber-secure digital decade for the EU,<br>2) Achieve a Security Union,<br>3) Strengthen the EU's position globally. |
| **Cyber Military Policy** | | |
| **2020 Indian Defence Cyber Agency.**<br>1) International offensive and defensive capabilities of the states;<br>2) Combat international cyberattacks using Cyber Warfare | **1947-Department of Defence (DoD)**<br>It secures cyberspace and helps to mitigate the risks to national security.<br><br>**2019 National Defense Authorisation Act.**<br>1) Reform the U.S. Government's Structure and Organisation for Cyberspace.<br>2) Strengthen norms and non-military tools.<br>3) Promote national resilience.<br>4) Reshape a safer cyber ecosystem.<br>5) Operationalise cybersecurity collaboration with the private sector<br>(6) Employ the military instrument to deter cyberattacks | **2004 ENISA**<br>First EU *Cybersecurity* Act (in force since June 2019)<br><br>**2004 European Defense Agency**<br>Military mobility programs and international cooperation in armed forces and cybersecurity domain<br><br>**2014 Cyber Defence Policy.**<br>1) Support the development of member states' cyber defence capabilities related to CSDP.<br>2) Enhance the protection of CSDP;<br>3) Promote civil-military cooperation with wider EU cyber policies;<br>4) Improve training, education, and exercises opportunities; and<br>5) Enhance cooperation with relevant international partners. |

European security policy has been changing in critical ways.[56] The old threats involving armour from the East have been replaced by invisible enemies whose origin is rarely identifiable. Considering how technologically dependent societies have become, cyberattacks pose a threat to critical infrastructure, personal data, financial and governmental institutions. According to Bendiek, this is "one of the key challenges to security policy in the 21st century".[57]

The EU must adapt its strategies and policies to this new security challenge. Ironically, this must occur in a moment when conventional EU defence cooperation finally appears to be advancing.[58] Over decades of attempts to put through a defence cooperation alongside other European policies, the cautious establishment of the CSDP and its alterations through subsequent revisions of the 1992 Maastricht Treaty, it is now possible to notice new, long term initiatives, structures, and processes, such as the establishment of the PESCO by the European Council in December 2017.

This new security scenario can be quite challenging for the EU. States like the US, for instance, hinges on its own foreign and domestic policies, the legal and budgetary power of a central government, and its unified military framework for both the elaboration and implementation of cyber defence policies and capabilities. The EU, by contrast, is beholden to member states, each responsible for developing its own cybersecurity framework. This, combined with multiple levels of priorities, capabilities, threats, and cyber maturity, causes an inconsistent and fragmented approach to the ultimate impacts of cyberspace, as well as putting the EU in a much more precarious position vis-à-vis cyber capacity building.

That said, this chapter will identify and discuss the most oft-cited policy and legal challenges for developing EU cyber capabilities. Note, however, that this subject warrants a more extended discussion than we can here give it and, therefore, this study is not to be considered exhaustive. Furthermore, taking into consideration the ever-increasing pace of technological innovation, new challenges may emerge, and extra complexity may compound previously existing ones.

The first challenge relates to governments' perspectives of cybersecurity. Some of the member states, such as Germany and the Netherlands, regard cybersecurity as a matter of homeland security. Others, including Latvia and Denmark, treat it as a defence issue, while still others, such as Finland and Italy, deem cybersecurity as a commerce and communication concern.[59] This discrepancy in perception becomes a major hindrance when it is time to (further) develop a unified legal framework for cyberspace.

The second challenge is the balancing act between the EU prerogatives and the member states' sovereignty. Even though defence matters are mainly within the responsibilities of member states, the EU is in charge of the common security and defence, which "is an integral part of the Union's common foreign

56. Annegret Bendiek, "European Cyber Security Policy", October 2012, SWP Research Paper 13/2012, Stiftung Wissenschaft und Politik, p. 5.
57. Ibid.
58. Ramses A. Wessel, "Cybersecurity in the European Union: Resilience through Regulation?", Routledge Handbook of EU Security Law and Policy (Routledge, 2019), p. 283.
59. Luukas K. Ilves et al., "European Union and NATO Global Cybersecurity Challenges: A Way Forward", PRISM, Vol. 6, No. 2, p. 132.

and security policy".[60] Nevertheless, as Röhrig and Smeaton notes, "[w]ithin the EU there is often a discussion between M[ember] S[tates] and the Institutions about what constitutes EU business, and what is sovereign, and therefore national business".[61] Thus, several European countries, like the Netherlands, France, and Belgium, have created their own NCSS' to cope with cybercrime and promote social-economic benefits from the cyber domain. It is perhaps useful to underline that some member states "have included a military perspective of cyber-defence in their national approaches" while others have only mentioned defence objectives.[62] However, this patchwork of domestic policies not only is not effective enough to address threats posed by cyberspace but also undermines broader EU political and economic interests.

A third challenge for developing cyber capabilities is the complex array of mandates within EU institutions and bodies. At the EU level, there is an intricate operational structure vis-à-vis who is responsible for cyber-defence activities, such as detection, reaction, and response. These tasks are divided between the EEAS, General Secretariat of the EU Council, and the European Commission.[63] It is not unreasonable to assume that this well-established and elaborate system would be regarded as a positive aspect of the EU cyberinfrastructure. Unfortunately, not rarely the mandates within EU institutions still echo the old three-pillar system, further compounding efforts at cooperation.[64] According to the 2014 EU Cyber Defence Policy Framework, there is "a need to streamline security rules for the information systems provided by different EU institutional actors during the conduct of CSDP operations and missions. In this context, a unified chain of command should be considered to improve the resilience of networks used for CSDP".[65]

The fourth challenge is the uncertainty regarding the application of some international rules to the cyber domain. In the 2014 Wales Summit, the North Atlantic Council[66] affirmed that "cyber defence is part of NATO's core task of collective defence"[67], and in the 2016 Warsaw Summit it recognised "cyberspace as a domain of operations in which NATO must defend itself as effectively as it does in the air, on land, and at the sea".[68] Despite the acknowledgement of cyberspace as a domain of military operations, there remains several legal issues to be addressed. As observed by Pawlak, the "issue of militarisation and expansion of cyber weapons is problematic given the lack of clarity on when a cyberattack would constitute use of force under Article 2.4 of the United Nations Charter and the threshold for self-defence, as stipulated in Article 51.3".[69] Accordingly, Sommario states that when cyber threats "may degenerate into an armed conflict, the exercise for international lawyers becomes that of assessing whether the existing legal framework […] offers adequate rules to protect states and indi-

60. Jérôme Legrand, "Common security and defence policy", November 2019, European Parliament. Available at: https://europarl.europa.eu/factsheets/en/sheet/159/common-security-and-defence-policy.
61. Wolfgang Röhrig and Rob Smeation, "Cyber Security and Cyber Defence in the European Union: Opportunities", Synergies and Challenges, Cyber Security Review Summer 2014, p. 25.
62. Carmen-Cristina Cîrlig, "Cyber defence in the EU: Preparing for cyber warfare?", October 2014 European Parliamentary Research Service, p. 6.
63. Neil Robinson et al., "Stocktaking study of military cyber defence capabilities in the European Union (milCyberCAP)", RAND Corporation, 2013, p. 6. Available at: https://www.rand.org/pubs/research_reports/RR286.html.
64. The three pillars are: the European Communities, the Common Foreign and Security Policy and Police and Judicial Cooperation in Criminal Matters.
65. Council of the European Union, EU Cyber Defence Policy Framework November 18, 2014, p. 6. Available at: https://www.europarl.europa.eu/meetdocs/2014_2019/documents/sede/dv/sede160315eucyberdefencepolicyframework_/sede160315eucyberdefencepolicyframework_en.pdf.
66. The North Atlantic Council is the main political decision-making body within the North Atlantic Treaty Organisation.
67. The North Atlantic Council, *Wales Summit Declaration*, September 5, 2014, para. 72. Available at: https://www.nato.int/cps/en/natohq/official_texts_112964.html.
68. The North Atlantic Council, *Warsaw Summit Communiqué*, July 9, 2016, para. 70. Available at: https://www.nato.int/cps/en/natohq/official_texts_133169.htm.
69. Patryk Pawlak, "Cyber Diplomacy: Confidence-building measures", European Parliamentary Research Service, October 2015, PE 571.302, p. 2. Available at: https://www.europarl.europa.eu/RegData/etudes/BRIE/2015/571302/EPRS_BRI(2015)571302_EN.pdf.

viduals from the menaces of cyber warfare".[70] Note that, despite the attempt of both state and non-state driven initiatives[71] to provide much-needed clarity to some grey areas of international cyber law, many uncertainties remain vis-à-vis the application of the current legal framework to the cyber domain, which complicates the implementation of an effective EU cyber framework.

A fifth factor that underlines the challenges for developing EU cyber capabilities is the dearth of unanimously agreed definitions or a taxonomy of cyber-related terms. Considering that the principal building blocks of the Internet were laid more than two decades ago, neither the international community nor the EU, were able to come to an agreement regarding the definition of several terms. As regarded by Cîrlig, "terms such as cybersecurity, cyberattack, cybercrime, cyberwar (or warfare) and cyberterrorism have entered the public discourse; however, there is no consensus on their definitions, making it difficult to create a conceptual framework in which relations and international agreements related to cyberspace can be developed".[72]

The final challenge is both the amount and diversity of actors involved in cybersecurity, which may result in overlap of work and an incoherent approach towards the discussion and formulation of cyber policies. Whether at domestic, EU, or international level, it is possible to find several actors participating in the development of cyber policies. This includes governmental agencies, academia, private industries, and international organisations. At the domestic level, governments must work alongside law enforcement and intelligence agencies, universities, research centres, as well as relevant ICT companies. The weight of each of these actors varies from one member state to another according to their goals, threat perception, interests, and available resources. This makes a consistent approach at the EU level harder to achieve. Certainly, this situation is aggravated if one takes into consideration the complex array of mandates within the EU institutions and bodies already extant.

Still regarding the number of actors in cyberspace, in order to develop cyber defence capabilities, the EU must engage with international organisations and multinational Centres of Excellence that are active in the field, such as NATO, the African Union, or the Organization for Economic Cooperation and Development (OECD).[73] Cooperation with international partners is, according to the EU Cybersecurity Strategy, crucial to "ensure effective defence capabilities, identify areas for cooperation, and avoid duplication of efforts".[74] The EU must collaborate with third countries, especially those sharing its values. In doing so, the EU will achieve a "high level of data protection, including for transfer to a third country of personal data".[75] In addition, cooperation with the private sector is necessary to achieve an effective cybersecurity framework.

As observed by Verhelst, "cyberspace is a domain in which industry and the private sector play a pivotal role".[76] Indeed, ICT companies

70. Emanuele Sommario, "Applying the jus in bello in the cyber domain: Navigating between lex lata and lex ferenda", 2016, QIL, p. 14. Available at: https://www.qil.org/applying-jus-bello-cyber-domain-navigating-lex-lata-lex-ferenda/.
71. The most important state initiative regarding the application of international law to cyberspace is the UN Governmental Group of Experts on Developments in the Field of Information and Telecommunications, which between 2004 and 2015 submitted three reports. The leading non-state driven initiative is the Tallinn Project, which published two editions of the Manual in 2013 and 2017 under the auspices of the NATO Cooperative Cyber Defence Centre of Excellence (NATO CCD COE).
72. Carmem-Cristina Cîrlig, "Cyber defence in the EU", European Parliamentary Research Service, October 2014, p. 2. Available at: https://www.europarl.europa.eu/RegData/etudes/BRIE/2014/542143/EPRS_BRI(2014)542143_REV1_EN.pdf.
73. High Representative of the European Union for Foreign Affairs and Security Policy, "Cybersecurity Strategy of the European Union", 2013, p. 15. Available at: https://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf.
74. Ibid., p. 11-12.
75. Ibid., p. 15.
76. Anne Verhelst, "Cybersecurity and International Law: a closer look at recent UN and EU initiatives", KU Leuven, p. 6. Available at: https://lirias.kuleuven.be/retrieve/552260.

are responsible for technological innovations and expertise, as well as for minimising the chances and potential consequences of cyber conflict by implementing "rigorous processes, tooling, and training to securely develop, operate, and maintain ICT products and services".[77]

## CONFIDENCE BUILDING MEASURES

This chapter will focus on a possible solution applicable to the military domain, regarding cybersecurity within the EU: Confidence-Building Measures (CBMs). CBMs not only function as mechanisms to establish "rules of the road" in cyberspace, the application of international law and norms of responsible state behaviour also function. To ensure clarity of argument, we will first define CBMs, then delve into the military cyber domain and explain which measures may apply in conflict situations.

### Military Confidence-Building Measures

Many political and military security axioms changed during the post - Cold War period. A period marked by confrontation and division which required the right measures to avoid escalation. CBMs were created to serve this goal. The function of these measures was to reinforce stability in a frozen status quo and reduce the risk of war in Europe.[78] However, it was not until 1975 when the foundations for the development of CBMs were formalised through the Helsinki Final Act. Naturally this generation of CBMs were designed for armed forces in Europe.[79] At subsequent meetings in Stockholm (1986) and Vienna (1990), states agreed on CBMs which resulted in the adoption of "militarily significant, politically binding, and verifiable confidence-building measures" and in a dialogue aiming a new set of negotiations on confidence and security-building measures (CSBMs), respectively.[80] [81]

Despite these politically binding acts, no specific definition on CBMs has ever been agreed upon.[82] Certain experts define CBMs as an "instrument of international politics, negotiated by, and applied between states" whose aim is "to prevent the outbreak of an (international) armed conflict or hostilities, to avert escalation and to reduce military tension by building up mutual trust between States and by increasing transparency and predictability."[83] [84] [85] The Confidence and Security Building Measures Working Group of the Council for Security Cooperation in the Asia - Pacific (CSCAP) stated that CBMs include "formal

77. Angela McKay et al., "International Cybersecurity Norms: Reducing conflict in an Internet-dependent world", 2015, Microsoft, p. 15.
78. Zdzislaw Lachowsku, "Confidence-Building Measures'", Stockholm International Peace Research Institute.
79. Richard E. Darilek, "Confidence-Building: Defusing the Cold War in Europe" p. 249 – 260.
80. "Arms Regulation and Disarmament - Confidence-building measures", available at https://www.nationsencyclopedia.com/United-Nations/Arms-Regulation-and-Disarmament-CONFIDENCE-BUILDING-MEASURES.html#ixzz6jhnSHsT4
81. Document of the Stockholm Conference on Confidence - and Security-Building Measures and Disarmament in Europe, U.S department of State "CSBMs were designed to increase openness and predictability about military activities in Europe, with the aim of reducing the risk of armed conflict in Europe."
82. Pieter van Dijk, "The Implementation of the Final Act of Helsinki: The Creation of New Structures or the Involvement of Existing Ones?", 1989, Michigan Journal of International Law Volume 10 Issue 1, said regarding this statement that "The conclusion that the Final Act is not a legally binding agreement does not mean that the matters agreed upon between the participating states, and laid down in the Final Act, should not be binding. […] In conclusion it may be stated that the Final Act contains many binding commitments, several of which are even legally binding, although the Act itself does not have the character of a legally binding agreement."
83. Zdzislaw Lachowsku, "Confidence-Building Measures'", NATO Cooperative Cyber Defence Centre of Excellence.
84. United Nations, "Military Confidence-building. Available at: https://www.un.org/disarmament/convarms/cbms/
85. Zagoria, Donald S. and Fugarino Chris, "Breaking the China – Taiwan Impasse", 2003, Greenwood, p. 158

and informal measures, whether unilateral, bilateral or multilateral, that address, prevent, or resolve uncertainties among states, including both military and political elements."[86]

Some state CBMs were not just created to prevent war but also "to reduce the possibilities for surprise attack, and even, if possible, in the ability to use military forces for the purpose of political intimidation".[87] Others agree on this, but add that CBMs exist to: 1) prevent escalation through conciliatory moves and negotiations where parties would work together to build confidence to enter into deadly conflict; and 2) to consolidate the process and its outcomes through measures such as power sharing, electoral reform, and power decentralisation which foster political inclusion and allow for political exchange and learning among parties in conflict.[88] [89]

Since their conception, CBMs have been central to military cooperation and conflict resolution. According to Neukirch, "[t]he basis of current arrangements to ensure transparency and build trust between participating States."[90] Examples of international success following the implementation of CBMs, include the Korean conflict; the Pakistan-India conflicts and the Taiwan-Popular Republic of China.[91] [92] [93] In Europe, we find the Moldova-Transnistria case and the Kosovo conflict.[94] [95]

Some measures emerging from these conflicts include:

1) Declaratory Statements: Both sides publicly express their intentions to resolve disputes peacefully and eventually sign a joint statement ending hostilities.

2) Operational Military Constraints. States unilaterally affirm they will refrain from flying military aircraft across a centreline. Another step could be unilateral declarations to keep a certain distance from a centreline; in effect creating a "no-fly zone".

3) Military Exchanges. Visits by former military officers and civilian national security experts. These could be regularised and expanded to include active-duty officers as trust increases.

4) Conflict Avoidance Arrangements. Negotiated agreements to prevent dangerous military activities. Such an agreement would include codes of conduct for military forces and mandated modes of consultation and communication in crises.

However, the application of CBMs must be tailored to the distinctive geographical, political, and cultural environments in each region or situation and must always respect the sovereignty of the nation[96].

Other solutions may apply if we consider various EU challenges explained above:

- Build Cyber Defence Capabilities within EU member states. Member states, EU institutions and European agencies should enhance cooperation in the field of cyber defence capabilities by assisting each other.
- Build a common EU Cyber Defence Policy framework. Member states should join efforts

86. Glosserman, Brad, "Cross Strait Confidence Building", February 2005, issues & Insights Vol. 5 No. 2
87. Ibid 87.
88. Mason, Simon J. A. and Siegfried, Matthias, "Confidence Building Measures (CBMs) in Peace Processes", 2013, African Union and the Centre for Humanitarian Dialogue, Volume 1, p. 57-77.
89 Ibid.
90. Claus Neukirch, "Confidence building in the OSCE", September 2012.
91. Irshad, Muhammed, "Indo-Pak Confidence-Building Measures", August 2002, Defence Journal, available at http://www.defencejournal.com/2002/august/confidence.htm
92. Zdzislaw Lachowski, et al., "Tools for building confidence on the Korean peninsula", International Peace Research Institute (SIPRI). They state "Bilateral tension has also often been high between North Korea and the USA; and China, Japan, and Russia are involved in the complex security situation on the Korean Peninsula.
93. Ibid 83.
94. Nino Kemoklidze & Stefan Wolf, "Trade as a confidence-building measure in protracted conflicts: the cases of Georgia and Moldova compared", December 12, 2019, Eurasian Geography and Economics. Available at:https://www.tandfonline.com/doi/pdf/10.1080/15387216.2019.1702567?needAccess=true
95 Prishtina, "Kosovo serbs after the declaration of independence. The right momentum for confidence building measures", July 2008, Kosovar Institute for Policy Research and Development. Available at:http://www.kipred.org/repository/docs/Kosovo_Serbs_After_the_Declaration_of_Independence-_The_Right_Momentum_for_Confidence_Building_Measures_876393.pdf
96. Bonnie S. Glaser, "Cross-Strait Confidence Building: The Case for Military Confidence-Building Measures", 2003.

to establish a solid legal framework in the cyberconflict domain.
- Promote civil-military dialogue at EU and international level. The European Council stated, "with a view to promoting the EU political, economic and strategic interests, the EU launched cyber dialogues with China, India, Japan, South Korea and the United States."
- Launch dialogue with international partners. This dialogue and cooperation should exploit synergies and work closely in the field of cyber defence. Public and private sectors should work more closely to further develop cyber defence technologies and enhance cyber defence in general.

## Applicability of military CBMs in the cybersecurity domain

As cyberspace is increasingly (mis)used by states for military purposes, international negotiations on rules of behaviour, cybersecurity CBMs have evolved. Consequently, cyberspace has become an element in debates at the global and regional levels. If we accept that cybersecurity is the fifth military domain, it is thus subject to issues that are both regulated and unregulated.[97]

Innovation and geopolitical dynamics have propelled states to form confidence-building measures to create arms control regimes and to institutionalise constraints on offensive military technology. Yet, as Pawlak states, "the risk is […] that the progressing militarisation of cyberspace [...] will accelerate the cyber arms race", thus increasing the risk of escalation and conflict. The question arises "to what extent cyber CBMs can be used to mitigate the risks to stability between cyber powers?"[98]

The CBM debate in the field of cybersecurity has resulted in the creation of important platforms enabling governments to converse on these issues. The Organisation for Security and Cooperation in Europe (OSCE) adopted two sets of cyber-related confidence-building measures to strengthen cybersecurity. The first established official Points of Contact (PoC) and lines of communication to prevent possible tensions resulting from cyber activities. The second focuses on further enhancing cooperation between OSCE participating states. It includes effective mitigation of cyberattacks on critical infrastructure, and the military domain; greater transparency in military budgets, strategic doctrine, and legal interpretations.[99]

As Pawlak reminds "[w]ith cybersecurity attracting increasing interest and the barriers for access to cyber capabilities decreasing, the risk of a conflict resulting from misunderstandings and miscalculation is growing." To counter the difficulty of attribution and the protection of cyberspace, CBMs stand out as a key tool in preventing and reducing the risk of a conflict.[100]

Legally, there is no solid legislation regulating CBMs. The United Nations General Assembly Resolution 65/63 of 2011, distinguishes three categories of military CBMs:

1) Communication and information exchange; aimed at fostering better understanding of national military capabilities and activities, where military manoeuvres and movements are notified via diplomatic channels in which States should take part.

97. Kasapoglu Can, "Cyber Security: Understanding the Fifth Domain Author(s)", 2017, Centre for Economics and Foreign Policy Studies.
98. Erica D. Borghard and Shawn W. Lonergan, "Confidence Building Measures for the Cyber Domain Source: Strategic Studies Quarterly", 2018, Air University Press, Vol. 12, No. 3, pp. 10-49.
99. OSCE Secretariat, "OSCE participating States, in landmark decision, agree to expand list of measures to reduce risk of tensions arising from cyber activities", March 2016. Available at: https://www.osce.org/cio/226656
100. Leandro Mendes Pereira, "Understanding Cybercrime: Current threats and responses", Finabel.org, pp 9-15 . Available at: https://finabel.org/wp-content/uploads/2020/12/Understanding-cybercrime-15.12-1.pdf

2) Transparency and verification measures; including exchange of documents (e.g., military doctrines), exchange of observers, military data exchange or pre-notification of military movements or exercises.[101]

These options come from the necessity to build confidence through use of "hotlines" which help to improve communication and prevent crises.[102] [103]

3) Military restraint measures implemented to limit the capacity of parties for (surprise) offensive attacks.[104]

Advanced CBMs could include measures that prevent the emplacement of large numbers of troops and weapons in specific zones, thus limiting the ability to mount large-scale offensives. Restrictions could be set on the types, scale, frequency, and timing of military exercises. Both sides could agree to prohibit exercises in important air, land and sea routes and at sensitive political junctures.

In 2013, the OSCE adopted the Istanbul Declaration, supplemented by a resolution dedicated to cybersecurity. It launched cybersecurity confidence-building measures to "enhance interstate cooperation, transparency, predictability and stability and to reduce the risks of misperception, escalation and conflict that may stem from the use of ICT" and to promote a culture of cybersecurity.[105]

CBMS, are ultimately, activities that not only aim to promote understanding between nations, but also improve cybersecurity capabilities. While the pursuit of offensive technology in cyberspace may be unavoidable, nations should be encouraged to prioritise investments in defence. For example, the US and other countries have been investing in offensive and defensive cyber capabilities of a military nature. Considering the reliance on ICTs for the delivery of governmental, financial, and public services, states and public society are at severe risk for cyberattacks. Even more critically, states should engage with one another to a) share cybersecurity learnings and benefits; b) ensure their actions and intentions in cyberspace are not misinterpreted; and c) increase the role of deterrence in cyberspace.

Due to the constant development of IT and Artificial Intelligence (AI), cybersecurity has become a more complex and challenging domain lacking the laws to regulate it. As Yasmin states "[u]nfortunately the existing legal norms do not offer a clear and comprehensive framework within which states can shape policy responses to the threats of hostile cyber operations."[106] In any case, and concerning the field of cyber operations "small, initial steps could be taken in order to set a baseline for future transparency measures such as publishing a cybersecurity strategy".[107] More importantly, however, in Sander's words, "where there is no political will for negotiations, CBMs alone are unlikely to make the difference."[108]

101. Kristina Sander, "Confidence-Building Measures in Cyber", 2018, Institute for Security and Safety.
102. Jason Haley et al, "Confidence-building measures in cyberspace" says that "secure and resilient communication channel or a hotline that will function during and following a cyber crisis." 2014, Atlantic Council, National Defence College. Available at:https://www.atlanticcouncil.org/wp-content/uploads/2014/11/Confidence-Building_Measures_in_Cyberspace.pdf
103. Maisse Michelle, "Confidence-Building Measures" 2003. Available at:http://www.beyondintractability.org
104. Pawlak, Patryk, "Cyber diplomacy Confidence-building measures", October 2015, European Parliamentary Research Service.
105. Pawlak Patryk, "Confidence-Building Measures in Cyberspace: current debates and Trends", *International Cyber Norms,* Chapter 7.
106. Tughral Yamin, "Developing Information-Space Confidence Building Measures (CBMs) between India and Pakistan", June 2014, Sandia National Laboratories. Available at:https://prod-ng.sandia.gov/techlib-noauth/access-control.cgi/2014/144934.pdf
107. "Establishing Bilateral Confidence-Building Measures (CBMs) in Cyberspace between the United States and Russia", april 5, 2005. Available at https://tashajhangiani.com/2020/04/05/establishing-bilateral-confidence-building-measures-cbms-in-cyberspace-between-the-united-states-and-russia/
108 Ibid 100.

# CONCLUSION

Cybersecurity remains complex and unpredictable. Thus, it is difficult to foretell what issues might arise in future or what measures might ultimately offer the most utility in terms of stemming conflict.

States and non-state actors are progressively developing legal frameworks. Therefore it is likely that cyber operations will be covered by lawful treaties. Countries such as India or USA are far more experienced in the cybersecurity domain and should serve as examples for the EU, which lacks common legislation amongst its member states, especially regarding CBMs applicable to cybersecurity. Naturally, (cyber)warfare will change, the present dimensions will give way to new unknown dimensions where virtual combat could cause more damage than physical combat through the targeting of critical infrastructure.

Cyber operations applied to the military cyber domain will encompass both offensive and defensive operations. However, the problem of attribution, combined with the lack of legal instrumentation to regulate it should force the EU to act faster to strengthen cooperation between the member states. Bakowskin states "Cyberwar, and cyber defence have […] rarely been addressed at EU level [and] [M]ember [S]tates tend to cooperate within NATO instead to improve their cyber-defence capacities".

To foster cooperation, one solution proposed is the inclusion of CBMs. These measures specifically focused on the military and strategic approach, allow for resolution through dialogue or common practices. As Frye has stated, "[w]e have invented our way into unprecedented insecurity through technological innovation. We must invent our way out of it through political innovation. In that endeavour, confidence-building measures are likely to prove indispensable tools."

It is important to stress that solutions must be adopted to fill the legal gaps in the field of cybersecurity. It would reduce tensions and increase international co-operation; however, such measures cannot be taken in isolation under any circumstance.[109] Now, it is time for Europe to work together on concrete actions to secure our cyber system.

# BIBLIOGRAPHY

Aaron P. Brecher, "Cyberattacks and the covert action statute: towards a domestic legal framework for offensive cyberoperations", Michigan Law Review, vol. 111.

Aditi Agrawal, "India's Cybersecurity Strategy Policy in 2020", June 22, 2019. Avail-

109. Cybersecurity Tech Accord joins the UN dialogue to limit the offensive use of digital technologies, December 6, 2019 . Available at: https://cybertechaccord.org/cybersecurity-tech-accord-joins-the-un-dialogue-to-limit-the-offensive-use-of-digital-technologies/

able at: https://www.medianama.com/2019/06/223-indias-cybersecurity-strategy-policy-in-2020-says-national-cybersecurity-coordinator-rajesh-pant/

Andrew Huckle, "The Evolution of the European Union's Common Security and Defence Policy", E-International relations. Available at: https://www.e-ir.info/2016/07/07/the-evolution-of-the-european-unions-common-security-and-defence-policy

Angela McKay et al., "International Cybersecurity Norms: Reducing conflict in an Internet-dependent world", 2015, Microsoft.

Anegret Bendiek, "European Cyber Security Policy", October 2012 SWP Research Paper Stiftung Wissenschaft und Politik.

Anne Verhelst, "Cybersecurity and International Law: a closer look at recent UN and EU initiatives", KU Leuven, p.17 Available at: https://lirias.kuleuven.be/retrieve/552260.

Bonnie S. Glaser, "Cross-Strait Confidence Building: The Case for Military Confidence-Building Measures", 2003.

Bonnie S. Glaser, "Military Confidence-Building Measures: Averting Accidents and Building Trustin the Taiwan Strait", American Foreign Policy Interests, 2005.

Brad Glosserman, "Cross Strait Confidence Building", February 2005, issues & Insights Vol. 5 No. 2.

Carmen-Cristina Cîrlig, "Cyber defence in the EU: Preparing for cyber warfare?", October 2014, European Parliamentary Research Service.

Challenges to effective EU Cybersecurity policy, European Court of Auditors, 2019

Cherian, Munish, "Securing Cyberspace: International and Asian Perspectives", 2016, Pentagon Press.

Claus Neukirch, "Confidence building in the OSCE", 24 September 2012. Available at https://www.osce.org/secretariat/106440

Chris Kennedy, Three Major Gaps in the Cyberspace Solarium Commission's Report that need to be addressed, 2020. Available at: https://www.helpnetsecurity.com/2020/07/09/cyberspace-solarium-commissions-report/

Crowther, "National Defense and the Cyber Domain", 2018, The Heritage Foundation.

Divij Joshi, "A comparison of legal and regulatory approaches to cyber security in India and the United Kingdom", November 12, 2017 The Centre for Internet & Society.

Emanuele Sommario, "Applying the jus in bello in the cyber domain: Navigating between lex lata and lex ferenda", 2016. Available at: https://www.qil.org/applying-jus-bello-cyber-domain-navigating-lex-lata-lex-ferenda/

Erica D. Borghard and Shawn W. Lonergan, “Confidence Building Measures for the Cyber Domain Source: Strategic Studies Quarterly”, 2018, Air University Press, Vol. 12, No. 3. pp. 10-49.

G. Alexander Crowther and Shaheen Ghori, “Detangling the Web: A Screenshot of U.S. Government Cyber Activity”, 2015, Joint Force Quarterly, Issue 78 , pp. 75–83. Available at: http://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-78/jfq-78.pdf

Helen Durham, “Cyber operations during armed conflict:7 essential law and policy questions” Available at: https://blogs.icrc.org/law-and-policy/2020/03/26/cyber-armed-conflict-7-law-policy-questions/.

Herbert S. Lin, “Offensive cyber operations and the use of force”. Available at: https://jnslp.com/wp-content/uploads/2010/08/06_Lin.pdf.

Irshad, Muhammed, “Indo-Pak Confidence-Building Measures”, August 2002, Defence Journal, available at http://www.defencejournal.com/2002/august/confidence.htm

Jason Haley et al, “Confidence-building measures in cyberspace”, 2014, Atlantic Council, National Defence College. Available at: https://www.atlanticcouncil.org/wp-content/uploads/2014/11/Confidence-Building_Measures_in_Cyberspace.pdf

Jérôme Legrand, “Common security and defence policy”, November 2019, European Parliament,. Available at: https://europarl.europa.eu/factsheets/en/sheet/159/common-security-and-defence-policy.

Kasapoglu Can, “Cyber Security: Understanding the Fifth Domain”, 2017, Centre for Economics and Foreign Policy Studies.

Kristina Sander, “Confidence-Building Measures in Cyber”, 2018, Institute for Security and Safety.

Leandro Mendes Pereira, “Understanding Cybercrime: Current threats and responses”, December 2020, pp 9-15. Available at: https://finabel.org/wp-content/uploads/2020/12/Understanding-cybercrime-15.12-1.pdf

Luukas K. Ilves et al., “European Union and NATO Global Cybersecurity Challenges: A Way Forward”, 2016, PRISM, Vol. 6, No. 2, pp. 126-141.

Maisse Michelle, “Confidence-Building Measures”, 2003. Available at: http://www.beyondintractability.org.

Mason, Simon J. A. and Matthias Siegfried, “Confidence Building Measures (CBMs) in Peace Processes”, 2013 Volume 1, African Union and the Centre for Humanitarian Dialogue, 57-77.

Max Smeets, ‘The Strategic Promise of Offensive Cyber Operations’, Strategic Studies Quarterly , Vol. 12, No. 3 (FALL 2018), pp. 90-113.

Mike Levine, "Russia Tops List of 100 Countries that Could Launch Cyberattacks on US," ABC News, 2017. Available at: https://abcnews.go.com/US/russia-tops-list%20-100-countries-launch-cyberattacks-us/story?id=47487188

Neil Robinson et al., "Stocktaking study of military cyber defence capabilities in the European Union (milCyberCAP)", 2013, RAND Corporation. Available at: https://www.rand.org/pubs/research_reports/RR286.html.

Nidhi Singh, "India's New Defence Cyber Agency", 2019. Available at https://www.mediana-ma.com/2019/05/223-indias-new-defence-cyber-agency-nidhi-singh-ccg-nlud/

Nino Kemoklidze & Stefan Wolf, "Trade as a confidence-building measure in protracted conflicts: the cases of Georgia and Moldova compared", December 12, 2019, Eurasian Geography and Economics. Available at https://www.tandfonline.com/doi/pdf/10.1080/15387216.2019.1702567?needAccess=true

Panagiotis Trimintzios et al., "Cybersecurity in the EU Common Security and Defence Policy (CSDP): Challenges and risks for the EU", European Parliamentary Research Service, Scientific Foresight Unit (STOA), 2017, p.94.

Patryk Pawlak, "Cyber Diplomacy: Confidence-building measures", European Parliamentary Research Service, October, PE 571.302, 2015. Available at: https://www.europarl.europa.eu/RegData/etudes/BRIE/2015/571302/EPRS_BRI(2015)571302_EN.pdf.

Patryk Pawlak, "Confidence-Building Measures in Cyberspace: current debates and Trends", International Cyber Norms, Chapter 7.

Pieter van Dijk, "The Implementation of the Final Act of Helsinki: The Creation of New Structures or the Involvement of Existing Ones? New Structures or the Involvement of Existing Ones?", 1989, Michigan Journal of International Law Volume 10 Issue 1.

Ramses A. Wessel, "Cybersecurity in the European Union: Resilience through Regulation?", Routledge Handbook of EU Security Law and Policy, 2019, pp. 283-300.

Richard E. Darilek, "Confidence-Building: Defusing the Cold Warin Europe" p. 249 – 260.

Robert Chesney, "The Cyberspace Solarium Commission Report: A Lawfare Series", March 11, 2020, available at https://www.lawfareblog.com/cyberspace-solarium-commission-report-lawfare-series

Saikat Datta, "Cybersecurity, Internet Governance and India's Foreign Policy: Historical Antecedents, Internet Democracy Project", 2016.

Tom Uren, Bart Hogeveen and Fergus Hanson, 'Defining offensive cyber capabilities', Australian strategic policy institute, available at: https://www.aspi.org.au/report/defining-offensive-cyber-capabilities.

Tughral Yamin, "Developing Information-Space Confidence Building Measures (CBMs)

between India and Pakistan", June 2014, Sandia National Laboratories. Available at: https://prod-ng.sandia.gov/techlib-noauth/access-control.cgi/2014/144934.pdf

Zagoria, Donald S. and Fugarino Chris, "Breaking the China – Taiwan Impasse", 2003, Greenwood, p. 15.

Zdzisław Lachowski, "Confidence-Building Measures", MPEPIL, NATO Cooperative Cyber Defence Centre of Excellence, Tallinn, Estonia.

Zdzisław Lachowski et al, "Tools for building confidence on the Korean peninsula", International Peace Research Institute.

Zdzisław Lachowski, 'Confidence-Building Measures', Stockholm International Peace Research Institute.

Wolfgang Röhrig and Rob Smeation, "Cyber Security and Cyber Defence in the European Union: Opportunities, Synergies and Challenges", 2014, Cyber Security Review.

## Decisions/treaties

Consolidated versions of the Treaty on European Union signed on the 7th of December 2012.

Council decision of 24 June 2014 on the arrangements for the implementation by the Union of the solidarity clause, July 1, 2014, OJ L 192, p. 53–58.

Council of the European Union, "EU Cyber Defence Policy Framework", 18 November 18, 2014. Available at: https://www.europarl.europa.eu/meetdocs/2014_2019/documents/sede/dv/sede160315eucyberdefencepolicyframework_/sede160315eucyberdefencepolicyframework_en.pdf

Document of the Stockholm Conference on Confidence - and Security-Building Measures and Disarmament in Europe

Cyberspace Solarium Commission Executive Summary, US, 2020.

EU Cyber Defence Policy Framework adopted 18 november 2014, nr. 15585/14.

EU Cyber Defence Policy Framework (2018 update) adopted on 19 November 2018, nr. 14413/18.

European Defence Agency, 'summary on cyber defence', available at https://www.eda.europa.eu/what-we-do/activities/activities-search/cyber-defence

Guidelines for the Protection of National Critical Information Infrastructure, point 2 Available at: https://nciipc.gov.in/documents/NCIIPC_Guidelines_V2.pdf

Joint communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of regions on Cybersecurity Strategy of the European

Union: An Open, Safe and Secure Cyberspace of 7 February 2013, JOIN (2013) 1 final.

National Cyber Strategy, US, 2018

The North Atlantic Council, "Wales Summit Declaration", 5 September 2014. Available at: https://www.nato.int/cps/en/natohq/official_texts_112964.html.

The North Atlantic Council, "Warsaw Summit Communiqué", 9 July 2016. Available at: https://www.nato.int/cps/en/natohq/official_texts_133169.htm.

United Nations, Charter of the United Nations, October 24, 1945, 1 UNTS XVI, available at: https://www.refworld.org/docid/3ae6b3930.html

United States, The White House, "Presidential Policy Directive 20: U.S. Cyber Operations Policy", 2012, available at http://fas.org/irp/offdocs/ppd/ppd-20.pdf

US JCS. Cyberspace Operations, No. 9.

US Cyber Command, No 21.

Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies

## Others

ICTY 15 juli 1999, Prosecutor v. Dusko Tadić, IT-94-1-AR72

Activation of Article 42(7) TEU France's request for assistance and Member States' responses', available at: https://www.europarl.europa.eu/RegData/etudes/BRIE/2016/581408/EPRS_BRI(2016)581408_EN.pdf

"Cybersecurity Tech Accord joins the UN dialogue to limit the offensive use of digital technologies"Reducing tensions in cyberspace by promoting cooperation", December 6, 2019, available at https://cybertechaccord.org/cybersecurity-tech-accord-joins-the-un-dialogue-to-limit-the-offensive-use-of-digital-technologies/

Cybersecurity in the EU Common Security and Defence Policy (CSDP), Challenges and risks for the EU. 67

Cybersecurity: Five "Keepers" in the Cyberspace Solarium Commission Report, August 20, 2020 available at https://www.heritage.org/cybersecurity/report/cybersecurity-five-keepers-the-cyberspace-solarium-commission-report

"Establishing Bilateral Confidence-Building Measures (CBMs) in Cyberspace between the United States and Russia", april 5, 2005. Available at https://tashajhangiani.com/2020/04/05/establishing-bilateral-confidence-building-measures-cbms-in-cyberspace-between-the-united-states-and-russia/

Created in 1953, the Finabel committee is the oldest military organisation for cooperation between European Armies: it was conceived as a forum for reflections, exchange studies, and proposals on common interest topics for the future of its members. Finabel, the only organisation at this level, strives at:

- Promoting interoperability and cooperation of armies, while seeking to bring together concepts, doctrines and procedures;
- Contributing to a common European understanding of land defence issues. Finabel focuses on doctrines, trainings, and the joint environment.

Finabel aims to be a multinational-, independent-, and apolitical actor for the European Armies of the EU Member States. The Finabel informal forum is based on consensus and equality of member states. Finabel favours fruitful contact among member states' officers and Chiefs of Staff in a spirit of open and mutual understanding via annual meetings.

Finabel contributes to reinforce interoperability among its member states in the framework of the North Atlantic Treaty Organisation (NATO), the EU, and *ad hoc* coalition; Finabel neither competes nor duplicates NATO or EU military structures but contributes to these organisations in its unique way. Initially focused on cooperation in armament's programmes, Finabel quickly shifted to the harmonisation of land doctrines. Consequently, before hoping to reach a shared capability approach and common equipment, a shared vision of force-engagement on the terrain should be obtained.

In the current setting, Finabel allows its member states to form Expert Task Groups for situations that require short-term solutions. In addition, Finabel is also a think tank that elaborates on current events concerning the operations of the land forces and provides comments by creating "Food for Thought papers" to address the topics. Finabel studies and Food for Thoughts are recommendations freely applied by its member, whose aim is to facilitate interoperability and improve the daily tasks of preparation, training, exercises, and engagement.

FINABEL
Quartier Reine Elisabeth
Rue d'Evere 1
**B-1140 BRUSSELS**

Tel: +32 (0)2 441 79 38 – GSM: +32 (0)483 712 193
E-mail: info@finabel.org

You will find our studies at **www.finabel.org**

European Army Interoperability Centre

www.linkedin.com/in/finabelEAIC @FinabelEAIC @FinabelEAIC

Responsible publisher: Mario BLOKKEN - Finabel Permanent Secretariat - QRE - Rue d'Evere,1 - B-1140 Brussels - +32 (0)2 441 79 38