RESEARCH IN FOCUS

EU-US Cybersecurity Policy Coming Together: Recommendations for instruments to accomplish joint strategic goals

Julia Schuetze

Stiftung Neue Verantwortung

November 2020

EU CYBER DIRECT
Supporting EU Cyber Diplomacy

This project is funded by the European Union.

Contents

Disclaimer

The content of this publication does not reflect the official opinion of the European Union. Responsibility for the information and views expressed therein lies entirely with the author.

Abstract

The need for more US–EU collaboration on cybersecurity policy has been identified by policymakers and diplomats from the EU and the US in their official Cyber Dialogues 2018 and 2019 as well as by international cybersecurity policy scholars. As the EU shapes its cybersecurity policies and fosters coordination among member states, cooperation at the EU level becomes more important to the US. EU–US cooperation to achieve shared policy goals such as prosecution and prevention of cybercrime has already resulted in implementing policy instruments together such as a joint exercise or information-sharing agreement specifically on cybercrime. Nevertheless, on a broader strategic level and with the focus on responses to malicious cyber-activities, concrete steps forward have been difficult to achieve in an environment where the EU and the US grapple with an ever-changing threat landscape that targets their values and ways of life and has made them focus on developing further their own processes and policy approaches in 2018–2020.

This paper sets out to find actions that the EU and US can implement together. It takes a practical approach by first identifying joint strategic goals and analysing the commonalities of EU and US cybersecurity policy. This allows a broader perspective on what the EU and US joint strategic goals really are, and what is feasible to do together. It is important to take account of the limitations and divergences that, as many others have pointed out, make cooperation difficult, but this paper uses them more as a means to find which instruments are actually feasible. Anyone who is interested to learn more about the EU and US, as well as those who are looking to find a way forward for transatlantic cooperation, will find glimpses of hope here and there in a policy field where it cannot be denied that the EU and US diverge as much as they converge.

Key takeaways on EU-US cooperation

- The intention of closer cooperation between the US and the EU to prevent, detect and react to malicious cyber-activities lacks a clear signal of what the joint strategic goal(s) of closer cooperation are.
- Joint strategic goals can be developed by first identifying shared goals and then analysing which shared goals would be better pursued together.
- The EU and US should focus on:
  - Assisting each other in improving resilience
  - Achieving a common understanding of threats and vulnerabilities
  - Improving cooperation mechanisms among a diverse set of stakeholders
  - Improving the cybersecurity workforce
- The EU and US have 32 instruments in common.
- Looking at past instruments implemented together gives an indication of what may be feasible in the future. Of the 32 instruments the EU and the US have in common, they have so far implemented only eight together.
- There are three prerequisites for joint implementation of instruments:
  - The need for specific joint strategic goals
  - The need for cooperation mechanisms supported by regular exchange
  - The need for own capacity and availability to contribute to the joint endeavour

- The limitation 'availability of instrument' eliminates 30 instruments from being considered for joint implementation, as it is hard to overcome in the short term.
- The limitation 'lack of capability' eliminates one instrument for joint implementation, i.e. the gathering and sharing of classified intelligence, for which the EU level relies on member states' capabilities.
- The limitation 'lack of political/legal authority' eliminates 12 instruments for joint implementation. It includes for example many foreign instruments such as sanctions, public attribution and demarchés, but also internal instruments that are passed through legal actions, such as incident reporting requirements or declaration of what constitutes a critical infrastructure.
- There is potential for the EU and the US to save resources by jointly implementing a certain instrument; for example, both countries do open-source analysis of threats and vulnerabilities that target companies that operate in the European market as well as the US market. The same information may be shared through different channels.
- The paper identifies 20 common instruments that are feasible to do together.
- Seven recommendations describe how the 20 instruments could be implemented jointly so that they address the joint strategic goals for responding to malicious cyber-activities:
  - Develop joint technical bulletins
  - Fund a process to develop joint automatic, standardised open-source threat and vulnerabilities intelligence-sharing solutions among like-minded countries
  - Practise joint strategic and political assessments of threats and explore responses in a cybersecurity policy simulation
  - Joint comparative study on effectiveness of instruments via the Transatlantic Cyber Policy Research Initiative (TCPRI)
  - Develop targeted exercises and trainings for different stakeholders
  - Set up liaison officers at State Department and Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA) as well as the European External Action Service (EEAS) and the European Union Agency for Cybersecurity (ENISA)
  - Work together on global guidelines/frameworks for cybersecurity skills development

Key takeaways on EU cybersecurity policy for US policymakers

- The EU, a supranational organisation, has been active in conducting cybersecurity policy using a diverse set of instruments—a total of 36 were identified.
- Setting parameters is a way for the EU to have some influence on how incident reporting is specifically implemented, by offering guidance. Nevertheless, most details on implementation are decided at member-state level.
- For non-EU countries such as the US, EU Council decisions are important because they show the common political position within the EU and that follow-up political decisions may be taken at EU level on the topic, rather than just by member states individually.

- Frameworks in general indicate that the EU works closely with member states on long-term goals and ultimately aims to harmonise the implementation of instruments as much as politically feasible.
- The EU is positioning itself as an information hub with the aim of achieving a common situational picture among stakeholders within the EU to enable joint responses or foster preventive measures and mitigation.
- The EU acts as a provider offering workshops, summits and platforms to meet, and facilitates studies and educational campaigns that include a diverse set of stakeholders. These instruments allow stakeholders from across the EU to work together on diverse cybersecurity (policy) issues.
- Overall, funding can be seen as another resource for the EU to support EU cybersecurity policy goals and/or achieve the implementation and use of certain instruments, such as training, sharing of information, development of best practices and guidelines or increasing awareness.

Key takeaways on US cybersecurity policy for EU policymakers

- The US federal institutions have been active in conducting cybersecurity policy using a diverse set of instruments defined as governmental interventions to achieve policy objectives: a total of 58 have been identified.
- In order to find vulnerabilities and threats and thereby improve cybersecurity of federal agencies and other stakeholders, the US uses innovative instruments, experimenting with activities that may be new and not (yet) used in other policy fields e.g. hackathons.
- The National Institute of Standards and Technology (NIST) framework, for example, is voluntary but NIST's compliance standards guide federal agencies and contractors to meet requirements mandated under the Federal Information Security Management Act (FISMA) and other regulations.
- The US provides services for assessing the cybersecurity level and making recommendations after the tests.
- In order to respond to malicious activity effectively, US federal agencies have set up different coordination platforms. Those can be ad-hoc groups, such as the Cyber Unified Coordination Group.
- In order to achieve a common situational picture, the US uses different instruments, for example guidelines on how to gather and share classified and open source information with internal and external stakeholders.
- Public attribution is used to alert internal actors such as companies about ongoing malicious activities. These alerts are usually accompanied by information to identify the actors and deploy defences.
- The John S. McCain National Defense Authorization Act shaped the US position on what constitutes the imposition of consequences, noting that all instruments of national power can be used in response to certain states.
- The US identifies countries that pose risks to US cybersecurity as an instrument to enable responses that aim to 'disrupt, defeat and deter cyber attacks'. The US will compete and persistently engage in cyberspace with countries identified as a risk, using instruments such as monitoring and offensive cyber operations.

- Cyber Command works in concert with other domestic agencies, each doing its part towards the overarching goals and assisting other departments' missions with their activities.

All in all, what the author aims to achieve with this paper is to show what could be possible to do together and a way to analyze EU and US cybersecurity policy comparatively by looking at the different instruments each applies.

1. Introduction

It is in the EU's strategic interest to retain and develop essential capacities in order to secure its digital economy, infrastructure, society and democracy. Similarly, the US is pursuing advances in cybersecurity that will thwart adversaries and strengthen public trust in information technology (IT) systems in order to preserve the Internet's growing social and economic benefits. Cybersecurity policy issues, especially in relation to cyber diplomacy, have gained importance.

The need for more US–EU collaboration on cybersecurity policy has been identified by policymakers and diplomats from the EU and the US in their official Cyber Dialogues 2018 and 2019[1] as well as by international cybersecurity policy scholars.[2] As the EU shapes its cybersecurity policies and fosters cooperation among member states, cooperation becomes more important to the US as responsibilities are moved to the EU level. To achieve shared cybersecurity policy goals such as prosecution and prevention of cybercrime, EU–US cooperation has already resulted in some joint activities, such as a joint exercise or information-sharing agreement specifically on cybercrime.[3] Nevertheless, on a broader strategic level and with a focus on responses to malicious cyber-activities, concrete steps forward have been difficult to achieve in an environment where the EU and the US grapple with an ever-changing threat landscape that targets their values and ways of life and has made them focus on developing further their own processes and policy approaches in 2018–2020.

This paper takes a practical approach by first identifying joint strategic goals and analysing the commonalities of EU and US cybersecurity policy. By first taking a wide and then a more concrete approach, it allows a broader perspective on what the EU–US joint strategic goals really are, and what it is feasible to do together. It is important to take account of the limitations and divergences that, as many others have pointed out,[4] make cooperation difficult, but this paper uses them more as a means to find which instruments are actually feasible. Anyone who is interested to learn more about the EU and US, as well as those who are looking to find a way forward for transatlantic cooperation, will find glimpses of hope here and there in a policy field where it cannot be denied that EU and US diverge as much as they converge.

In the end, the paper identified 20 common instruments that are feasible to do together and have potential in addressing the joint strategic goals that the author found.

[1] Office of the Spokesperson, *Joint Elements Statement on the Sixth U.S.-EU Cyber Dialogue*, U.S. Department of State, Washington, DC, 24 May 2019, https://www.state.gov/joint-elements-statement-on-the-sixth-u-s-eu-cyber-dialogue/.

[2] A few examples of papers that mention the need for increased EU–US cooperation in cybersecurity are: George Christou, 'Transatlantic Cooperation in Cybersecurity: Converging on Security as Resilience?,' in *Cybersecurity in the European Union: Resilience and Adaptability in Governance Policy*, ed. G. Christou (Basingstoke: Palgrave Macmillan, 2016); Julia Schuetze, 'How to Operationalise a Transatlantic Cyber Policy Research Initiative (TCPRI)', *EU Cyber Direct*, 30 September 2019, https://eucyberdirect.eu/content_research/1432/; Adina Ponta, 'Cyber Operations Against Medical Facilities During Peacetime,' *Lawfare*, 1 May 2020, https://www.lawfareblog.com/cyber-operations-against-medical-facilities-during-peacetime

[3] Europol, 'Operational Agreements,' 6 December 2001, https://www.europol.europa.eu/partners-agreements/operational-agreements?page=1.

[4] Thomas Renard, 'EU Cyber Partnerships: Assessing the EU Strategic Partnerships with Third Countries in the Cyber Domain,' *European Politics and Society*, vol. 19, no. 3 (2018), pp. 321–37; George Christou, 'Transatlantic Cooperation in Cybersecurity: Converging on Security as Resilience?'; Annegret Bendiek and Martin Schallbruch, 'Europe's Third Way in Cyberspace,' SWP, December 2019, https://www.swp-berlin.org/10.18449/2019C52/; Jeremy Fleming, 'EU, US Go Separate Ways on Cybersecurity,' *Euractiv*, 5 March 2013, https://www.euractiv.com/section/cybersecurity/news/eu-us-go-separate-ways-on-cybersecurity/; Jason Healey, 'The Implications of Persistent (and Permanent) Engagement in Cyberspace,' *Journal of Cybersecurity*, vol. 5, no. 1 (2019), tyz008, https://doi.org/10.1093/cybsec/tyz008 .

2. Definitions

To follow the analytical thought process of the paper, the definitions given in Table 1 are important. They combine theoretical thinking by public policy scholars with the inputs from cybersecurity policy experts that were given in a workshop led by the author.

Table 1. Definitions of terms used in the paper

Term	Definition
Instrument	The paper draws on the following definitions of 'instrument'. An instrument is a linkage between policy formulation and policy implementation. The intention in policy formulation is reflected in policy implementation through an instrument. Governing instruments are usually implemented to achieve policy targets but adjusted to social, political, economic and administrative concerns.[5] Hence "Policy instruments – tools used by governments to pursue a desired outcome."[6]. The application of appropriate instruments largely determines the policy's success.
Joint instrument	For the purposes of this paper a joint instrument is considered 'an action that the US and the EU take together in order to reach a joint strategic goal that addresses malicious cyber activities' that "aim at undermining the EU's integrity, security and economic competitiveness, with the eventual risk of conflict".[7] Actions that the US and EU take individually but are coordinated would not fall under this definition. Therefore, a reaction to a specific threat, vulnerability or major incident includes implementing a joint instrument, which is an intervention made by the public authorities that addresses a specific goal. For example: the EU and US have both identified countering cybercrime as a goal. To improve joint investigations, the US–EU Working Group on Cybersecurity and Cybercrime conducted a transatlantic anti-cybercrime exercise. In this case the establishment of the working group and the exercise are two joint instruments that are implemented to achieve the

[5] Mohammad Ali, 'Assessment of Policy Instruments,' in *Sustainability Assessment*, Mohammad Ali (New York: Academic Press, 2013), pp. 99–106.

[6] Definition by Paul Cairney. 'Policymaking in the UK: What Is Policy and How Is It Made?,' in *Policy and Policymaking in the UK* (Basingstoke: Palgrave, 2015), https://paulcairney.files.wordpress.com/2013/08/chapter-2-20-8-13-cairney-policy-policymaking-uk.pdf. Also see further analysis on policy instruments: Paul Cairney, 'What Is Policy and Policymaking?,' in *Understanding Public Policy: Theories and Issues*, Paul Cairney (London: Red Globe Press, 2020).

[7] Council of the EU, 'Cyber-attacks: Council Is Now Able to Impose Sanctions,' press release, 17 May 2019, https://www.consilium.europa.eu/en/press/press-releases/2019/05/17/cyber-attacks-council-is-now-able-to-impose-sanctions /.

	joint strategic goal of countering cybercrime, a malicious activity.
Governmental resources	The analysis applies Hood and Margetts' (2007) taxonomy of instruments[8] as a useful way to classify instruments and thereby understand better what the EU and the US do to achieve cybersecurity policy goals. An important aspect of the analysis is the description of what governmental resources are used to implement an instrument. All instruments identified are therefore analysed according to how the EU and the US have implemented them. This will reveal to what extent an instrument has limitations for joint implementation. Possible resources to implement the instruments are: The use of legislation to prescribe certain standards (authority) The use of a government's own capacity to build capabilities such as risk assessments (organisation) The use of its own strategic position to gather information on best practices (information) The use of money to fund research (treasury) The classification analyses the type of governing resource on which instruments rely. For example, when the implementation of the instrument 'sanctions' relies on a unanimous decision (legal/political authority) given by all member states, this can be a clear limitation for implementation of the instrument on an EU level by EU institutions, as the EU institutions cannot easily implement the instrument sanctions on their own, which in turn can have consequences for joint implementation of that instrument with the US. This is different with instruments that are supported by the resource organisation, which is the case for the instrument 'digital forensics capacities'. Here the EU-level institutions, in this case the European Cybercrime Centre (EC3) rely on their own capabilities, e.g. highly specialised technical and digital forensic support capabilities. This can mean that joint implementation of the instrument can be less restricted.
The EU	In this paper the EU means any institutions, organs, agencies and fora *on an EU level*.

[8] Christopher C. Hood and Helen Z. Margetts, *The Tools of Government in the Digital Age* (Basingstoke: Palgrave Macmillan, 2007).

The US	In this paper the US means any institutions, agencies and fora *on a US federal government level*.
Strategic goals	Policy objectives that the US and/or the EU aim to achieve in the context of tackling the challenge of malicious cyber-activities. They can be found in speeches, communications, and embedded in strategies or legislations.
Shared strategic goals	Shared strategic goals are the strategic goals that the EU and US clearly share. This means for example that the goals aim to reach similar objectives described in the strategies or communications.
Joint strategic goals	Joint strategic goals describe specifically what the EU and the US would work together on in comparison to just focusing on achieving those goals internally themselves. They are developed out of shared strategic goals.

3. Developing joint strategic goals

Prerequisite to the development of joint instruments is the identification of joint strategic goals. Therefore, the analysis firstly concentrates on what the EU and the US aim to achieve with their respective cybersecurity policies. Currently, the intention of closer cooperation between the US and the EU 'to prevent, detect, deter, and respond to malicious cyber activities'[9] lacks a clear signal of what the joint strategic goal(s) behind closer cooperation are. *For the implementation of joint actions, identifying and prioritising joint strategic goals has the benefit of making sure that the actions do actually address the joint strategic goals.*

This paper develops joint strategic goals in three practical steps:

- Mapping of main strategic goals the EU and US voice in their legislations and strategies and through communication
- Identification of shared strategic goals, i.e. the goals the EU and the US have in common
- Development of joint strategic goals out of the shared strategic goals. This is to clearly state which strategic goals the EU and the US could work on together as it would benefit them.

This process is important, because both the US and the EU have independently identified strategic goals for their responses to malicious cyber-activities in the strategies and policies that they unilaterally implement, some but not all of which they have in common. A joint strategic goal should not diverge from what each individually aims to achieve, hence the process helps to avoid putting forth strategic goals that may only be supported by one side.

3.1. Identification of EU and US strategic goals

Firstly, the main strategic goals of the EU and US are identified. Strategic goals are policy objectives that the US and/or the EU aim to achieve in the context of tackling the challenge of malicious cyber-activities. They can be found in speeches, in communications and embedded in strategies or legislations. In order

[9] Office of Spokesperson, Joint Elements Statement on the Sixth U.S.-EU Cyber Dialogue.

to do this, the paper used the main strategies and political positions/communications. For ease of reading, the tables summarise the main strategic goals of the EU and the US.

3.1.1. The EU's cybersecurity policy strategic goals

To summarise, the EU's strategic goals are very much focused on decreasing the EU's internal vulnerabilities by seeking to increase resilience[10] and cybersecurity. These strategic goals can also be found in the area of cyber diplomacy and the Common Foreign and Security Policy (CFSP), where the EU aims to ensure resilience to create joint incident responses or to increase coordination, cooperation and situational awareness among stakeholders. The thinking goes beyond the EU's internal stakeholders, highlighting that if other states are becoming more resilient, then the EU internally may also be better protected. Threat-focused goals—strategic goals that aim to influence threat actors—can be found in the cyber-diplomacy toolbox and in cybercrime policies. Here the EU aims to influence behaviour but with the goal of preventing conflict and achieving the stability of cyberspace as well as to prosecute and achieve effective law enforcement response. This means overall that any instrument chosen by the EU ultimately aims to promote security and stability in cyberspace through strategically increasing international cooperation, and to reduce the risk of misperception, escalation and conflict.[11] Table 2 highlights the EU's strategic goals briefly.

Table 2. EU's cybersecurity policy strategy and objectives[12]

Cybersecurity of institutions	Internal security/ protection of critical infrastructure and digital single market[13]	Cybercrime	Cyber diplomacy and CFSP	Defence policy: Common Security and Defence Policy (CSDP)
- Responses: 'set-up of a crisis response process'[14] and 'robust and effective structures to promote cybersecurity and	- 'substantially improve our cybersecurity'[17] - 'evenly high level of security of network and information systems across the EU'[18] - 'build our resilience, to drive technological	- 'effective law enforcement response focusing on detection, traceability and prosecution of cyber criminals is central to building	- 'Strong cyber resilience'[33] 'conflict prevention e.g. reduce the risk of misperception, escalation and conflict'[34]	- 'foster cyber defence research and innovation cooperation'[42] - 'deterrence through the Member States'

[10] High Representative of the Union for Foreign Affairs and Security Policy, 'Joint Communication to the European Parliament and the Council. Resilience, Deterrence and Defence: Building Strong Cybersecurity for the EU,' JOIN/2017/0450 Final, 13 September 2017, https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A52017JC0450

[11] Council of the EU, 'Cyber-attacks: Council Is Now Able to Impose Sanctions.'

[12] Table made by the author.

[13] High Representative of the Union for Foreign Affairs and Security Policy, 'Joint Communication to the European Parliament and the Council. Resilience, Deterrence and Defence.'

[14] European Commission, 'Annex to the Commission Recommendation on Coordinated Response to Large Scale Cybersecurity Incidents and Crises,' 13 September 2017, https://ec.europa.eu/transparency/regdoc/rep/3/2017/EN/C-2017-6100-F1-EN-ANNEX-1-PART-1.PDF

[17] High Representative of the Union for Foreign Affairs and Security Policy, 'Joint Communication to the European Parliament and the Council. Resilience, Deterrence and Defence.'

[18] European Commission, 'Directive on Security of Network and Information Systems, the First EU-Wide Legislation on Cybersecurity [Updated on 28/10/2019],' 28 October 2019, https://ec.europa.eu/commission/presscorner/detail/en/MEMO_18_3651

[33] High Representative of the Union for Foreign Affairs and Security Policy, 'Joint Communication to the European Parliament and the Council. Resilience, Deterrence and Defence.'

[34] General Secretariat of the European Council, 'Draft Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities ('Cyber Diplomacy Toolbox') – Adoption,' 7 June 2017, https://data.consilium.europa.eu/doc/document/ST-9916-2017-INIT/en/pdf.

[42] European Commission, 'State of the Union 2017 – Cybersecurity: Commission Scales up EU's Response to Cyber-Attacks.'

Cybersecurity of institutions	Internal security/ protection of critical infrastructure and digital single market[13]	Cybercrime	Cyber diplomacy and CFSP	Defence policy: Common Security and Defence Policy (CSDP)
to respond to cyber-attacks'[15] - Threat overview: 'assess the threats facing the Union'[16]	innovation, to boost deterrence, reinforcing traceability and accountability'[19] - 'enhance cybersecurity'[20] - 'improve the EU's preparedness'[21] - 'boost EU-level cooperation, knowledge and capacity'[22] - 'enhancing and strengthening their capability and preparedness to prevent, detect and respond to network and information security problems and incidents.'[23]	effective deterrence'[28] - 'harmonising aspects of criminal law in the area of cybercrime through the Budapest Convention'[29] - 'providing for criminal procedural tools needed for the investigation and prosecution of attacks against information systems through the Budapest Convention'[30]	- Stability of cyberspace[35] - Coordinated Response to Large Scale Cybersecurity Incidents and Crises[36] - Cooperation (effective response, shared situational awareness, public communication messages)[37] - Influencing behaviour of external actors – to deter and respond to cyber-attacks[38]	defence capability'[43] - 'Stronger cyber defence capabilities'[44]

[15] High Representative of the Union for Foreign Affairs and Security Policy, 'Joint Communication to the European Parliament and the Council. Resilience, Deterrence and Defence.'
[16] Council of the EU, Council Decision of 24 June 2014 on the Arrangements for the Implementation by the Union of the Solidarity Clause (2014/415/EU), https://eur-lex.europa.eu/eli/dec/2014/415/oj.
[19] European Commission, 'State of the Union 2017 – Cybersecurity: Commission Scales up EU's Response to Cyber-Attacks,' 17 September 2017, https://ec.europa.eu/commission/presscorner/detail/en/IP_17_3193.
[20] ENISA, 'NIS Directive.' ENISA, June 9, 2020. https://www.enisa.europa.eu/topics/nis-directive.
[21] European Commission, 'State of the Union 2017 – Cybersecurity: Commission Scales up EU's Response to Cyber-Attacks.'
[22] European Commission, 'Cybersecurity,' 25 August 2020, https://ec.europa.eu/digital-single-market/en/cyber-security.
[23] High Representative of the Union for Foreign Affairs and Security Policy, 'Joint Communication to the European Parliament and the Council. Resilience, Deterrence and Defence.'
[28] High Representative of the Union for Foreign Affairs and Security Policy, 'Joint Communication to the European Parliament and the Council. Resilience, Deterrence and Defence.'
[29] General Secretariat of the European Council, 'EU Lines to Take on Cybercrime Developments in the Framework of the UN,' 14 September 2018, https://data.consilium.europa.eu/doc/document/ST-12095-2018-INIT/en/pdf.
[30] General Secretariat of the European Council, 'EU Lines to Take on Cybercrime Developments in the Framework of the UN.'
[35] General Secretariat of the European Council, 'Draft Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities.'
[36] European Commission, 'Annex to the Commission Recommendation on Coordinated Response to Large Scale Cybersecurity Incidents and Crises.'
[37] European Commission, 'Annex to the Commission Recommendation on Coordinated Response to Large Scale Cybersecurity Incidents and Crises.'
[38] High Representative of the Union for Foreign Affairs and Security Policy, 'Joint Communication to the European Parliament and the Council. Resilience, Deterrence and Defence.'
[43] High Representative of the Union for Foreign Affairs and Security Policy, 'Joint Communication to the European Parliament and the Council. Resilience, Deterrence and Defence.'
[44] High Representative of the Union for Foreign Affairs and Security Policy, 'Joint Communication to the European Parliament and the Council. Resilience, Deterrence and Defence.'

Cybersecurity of institutions	Internal security/ protection of critical infrastructure and digital single market[13]	Cybercrime	Cyber diplomacy and CFSP	Defence policy: Common Security and Defence Policy (CSDP)
	- 'strategic cooperation and the exchange of information'[24] - 'help the EU retain and develop the cybersecurity technological and industrial capacities necessary to secure its Digital Single Market'[25] - 'increase the competitiveness of the EU's cybersecurity industry and turn cybersecurity into a competitive advantage of other European industries'[26] - 'closing the skills gap and avoiding a brain drain by ensuring access of the best talents to large-scale European cybersecurity research and innovation projects'[27] - Devise breakthrough solutions to the cybersecurity challenges	- 'fostering a fast and effective regime of international cooperation through the Budapest Convention[31]' - 'strengthen the law enforcement response to cybercrime in the EU', stated in the launch of the EC3 in 2013[32]	'strengthen its response to cyber-attacks'[39] international cooperation for 'open, free and secure cyberspace as well as [to] support efforts to develop norms of responsible state behaviour, apply international law and confidence building measures in cybersecurity'[40] - 'promote cyber resilience'[41]	

3.1.2. US cybersecurity policy strategic goals

To summarise, the US federal government cybersecurity policy goals and objectives focus, on the one hand, internally on the protection of critical infrastructure, federal network and the digital economy with the objective of American prosperity, which presumably can only be achieved through security. The

[24] European Commission, 'NIS Cooperation Group, Shaping Europe's Digital Future,' 24 July 2020, https://ec.europa.eu/digital-single-market/en/nis-cooperation-group.
[25] European Commission, 'Proposal for a European Cybersecurity Competence Network and Centre,' Shaping Europe's Digital Future, 19 September 2018, https://ec.europa.eu/digital-single-market/en/proposal-european-cybersecurity-competence-network-and-centre
[26] Council of the EU, 'EU to Pool and Network Its Cybersecurity Expertise – Council Agrees Its Position on Cybersecurity Centres,' press release, 13 March 2019, https://www.consilium.europa.eu/en/press/press-releases/2019/03/13/eu-to-pool-and-network-its-cybersecurity-expertise-council-agrees-its-position-on-cybersecurity-centres/
[27] European Commission, 'Proposal for a European Cybersecurity Competence Network and Centre.'
[31] General Secretariat of the European Council, 'EU Lines to Take on Cybercrime Developments in the Framework of the UN.'
[32] Europol European Cybercrime Centre – EC3, 'Cybercrime is One of the EMPACT Priorities, Europol's Priority Crime Areas, under the 2018–2021 EU Policy Cycle,' 10 August 2020, https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3.
[39] European Commission, 'State of the Union 2017 – Cybersecurity: Commission Scales up EU's Response to Cyber-Attacks.'
[40] European Commission, 'State of the Union 2017 – Cybersecurity: Commission Scales up EU's Response to Cyber-Attacks.'
[41] European Commission, 'State of the Union 2017 – Cybersecurity: Commission Scales up EU's Response to Cyber-Attacks.'

objectives in this part include increasing resilience, improving the cybersecurity workforce, IT security and innovation as well as achieving functioning detection of and responses to threats. Another set of goals is linked to national security aspects such as the preservation of peace more broadly, and to persistently engage, counter or deter states that perform malicious activities by collecting intelligence and preparing military capabilities. Table 3 highlights the US federal government's cybersecurity policy strategic goals.

Table 3. US federal government cybersecurity policy strategic goals and objective

National Security/Defence and Foreign Policy	Protection of government networks and critical infrastructure, digital economy
- 'disrupt, defeat and deter' malicious activity from states that risk US cybersecurity[45]	- 'strengthen the security and resilience of the nation's critical infrastructure through technical innovation'[53]
- 'continue to develop and pilot emerging capabilities, tools, and practices to more effectively detect and mitigate evolving threats and vulnerabilities in a timely fashion and ensure that our cybersecurity approaches are flexible and dynamic enough to counter determined and creative adversaries'[46]	- 'a more secure, coordinated, seamless, transparent, and cost-effective IT architecture that transforms data into actionable information and ensures dependable mission execution in the face of a persistent cyber threat'[54] - 'improve cybersecurity to federal departments, agencies'[55]
- 'increasing resiliency, defending forward, and persistently contesting and countering malicious cyber actors'[47]	- 'Combat Cybercrime and Improve Incident Reporting'[56]
- 'Collect intelligence and prepare military capabilities'[48]	- modernisation
- 'Preserve peace and security by strengthening the ability of the United States—in concert with allies and partners'[49]	- 'strengthening the workforce to help ensure we have skilled cybersecurity workers today and a strong pipeline of future cybersecurity leaders'[57]

[45] Robert Chesney, 'The 2018 DOD Cyber Strategy: Understanding "Defense Forward" in Light of the NDAA and PPD-20 Changes,' *Lawfare*, 31 October 2019, https://www.lawfareblog.com/2018-dod-cyber-strategy-understanding-defense-forward-light-ndaa-and-ppd-20-changes ; 115th Congress Public Law 115-232, 'John S. McCain National Defense Authorization Act for Fiscal Year 2019,' U.S. Government Publishing Office, https://www.govinfo.gov/content/pkg/PLAW-115publ232/html/PLAW-115publ232.htm.

[46] DHS, 'U.S. Department of Homeland Security Cybersecurity Strategy,' 15 May 2018, https://www.dhs.gov/sites/default/files/publications/DHS-Cybersecurity-Strategy_1.pdf

[47] DoD, 'Department of Defense Cyber Strategy 2018,' Department of Defence, 2018. https://media.defense.gov/2018/sep/18/2002041658/-1/-1/1/cyber_strategy_summary_final.pdf.

[48] DoD, 'Department of Defense Cyber Strategy 2018.'

[49] White House, 'National Cyber Strategy,' September 2018, https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf.

[53] DHS, 'Critical Infrastructure and Resilience,' Department of Homeland Security, 17 September 2020. https://www.dhs.gov/science-and-technology/critical-infrastructure-and-resilience

[54] DoD, 'DoD Digital Modernization Strategy: DoD Information Resource Management Strategic Plan FY19-23,' Homeland Security Digital Library, 12 July 2019. https://www.hsdl.org/?abstract.

[55] CISA, 'Securing Federal Networks,' Cybersecurity and Infrastructure Security Agency, DHS, 24 July 2020. https://www.cisa.gov/securing-federal-networks.

[56] White House. 'National Cyber Strategy.'

[57] National Initiative for Cybersecurity Careers and Studies, 'Cybersecurity Workforce Development Toolkit,' https://niccs.us-cert.gov/workforce-development/cybersecurity-workforce-development-toolkit

National Security/Defence and Foreign Policy	Protection of government networks and critical infrastructure, digital economy
- 'Expand American influence abroad to extend the key tenets of an open, interoperable, reliable, and secure Internet'[50] - 'defend the homeland by protecting networks, systems, functions, and data;'[51] - 'promote international commitments regarding behavior in cyberspace'[52]	- 'an organized and unified response to future cyber incidents'[58] - 'Promote American prosperity by nurturing a secure, thriving digital economy and fostering strong domestic innovation'[59]

3.2. Identification of shared strategic goals

These are the strategic goals that the EU and US *clearly* share. This means for example that the goals aim to reach similar objectives described in the strategies or communications. If unclear, the strategic goals are eliminated and not added to the shared goals. This means that, for example, goals are eliminated where it is not certain that they actually aim to reach the same objectives or the definition leaves too much room for ambiguity, e.g. deterrence. The EU aims to achieve deterrence through effective law enforcement response and increasing cyber-defence capabilities of member states as well as through diplomatic and political action with the ultimate goal to prevent conflict and reach cyber-stability: 'Cyber-attacks should be promptly investigated and perpetrators brought to justice, or action taken to allow an appropriate political or diplomatic response' and 'effective investigation and prosecution of cyber-enabled crime is a key deterrent to cyber-attacks', as well as 'building cybersecurity deterrence through the Member States' defence capability'.[60] The US strategy says that 'the administration will use 'all instruments of national power' to deter cyberattacks and impose 'swift and transparent consequences' against malicious actors.[61] It further states in the McCain Act 'that the United States should employ all instruments of national power, including the use of offensive cyber capabilities, to deter if possible'.[62] The US strategic goal of deterrence is not solely focused on cyber affairs: 'Pentagon leaders focused on deterrence, although not specifically cyber deterrence. Instead, they studied how cyberspace operations would factor into a broader deterrence effort.'[63] Hence, it is not clear whether the same 'strategic goal deterrence' objectives are followed by the EU and the US, even though they are named the same. Goals the EU and US clearly share are listed in Table 4.

[50] White House, 'National Cyber Strategy.'
[51] White House. 'National Cyber Strategy.'
[52] DoD, 'Department of Defense Cyber Strategy 2018.'
[58] White House, 'Presidential Policy Directive -- United States Cyber Incident Coordination,' National Archives and Records Administration, 26 July 2016, https://obamawhitehouse.archives.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident ; Andy Ozment and Tom Atkin, 'Critical Partnerships: DHS, DoD, and the National Response to Significant Cyber Incidents,' Department of Defense, 14 April 2015, https://dod.defense.gov/Portals/1/features/2015/0415_cyber-strategy/docs/DOD-DHS-Cyber_Article-2016-09-23-CLEAN.pdf.
[59] White House, 'National Cyber Strategy.'
[60] High Representative of the Union for Foreign Affairs and Security Policy, 'Joint Communication to the European Parliament and the Council. Resilience, Deterrence and Defence.'
[61] White House, 'National Cyber Strategy.'
[62] US Congress, 'FY2019 NDAA: Policy of the United States on Cyberspace, Cybersecurity, Cyber Warfare, and Cyber Deterrence,' July 2018, https://fas.org/sgp/news/2018/07/ndaa-1636.html.
[63] Mark Pomerleau, 'Is There Such a Concept as "Cyber Deterrence?",' *Fifth Domain*, 30 April 2019, https://www.fifthdomain.com/dod/2019/04/30/is-there-such-a-concept-as-cyber-deterrence/ .

Table 4. Strategic goals shared by the EU and the US

Shared Strategic Goals	US	EU
Cybersecurity and hardening systems	- 'defend the homeland by protecting networks, systems, functions, and data' - 'improve cybersecurity to federal departments, agencies'[64]	- 'substantially improve our cybersecurity'
Increasing resilience of key stakeholders	- 'strengthen the security and resilience of the nation's critical infrastructure through technical innovation'[65]	- 'Strong cyber resilience'
Gain threat overview	- 'Threat detection, collect intelligence, a more secure, coordinated, seamless, transparent, and cost-effective IT architecture that transforms data into actionable information and ensures dependable mission execution in the face of a persistent cyber threat' - 'more effectively detect and mitigate evolving threats and vulnerabilities in a timely fashion and ensure that our cybersecurity approaches are flexible and dynamic enough to counter determined and creative adversaries'	- 'assess the threats facing the Union' - 'strategic cooperation and the exchange of information'
Building capacity	- Building capacity among stakeholders such as local and state governments or critical infrastructure providers - 'strengthening the workforce to help ensure we have skilled cybersecurity workers today and a strong pipeline of future cybersecurity leaders'[66]	- Building capacity among EU's internal stakeholders (member states, public and private stakeholders, academia) - Contribute to closing the skills gap and to avoiding a brain drain by ensuring access of the best talents to large-scale research and innovation projects
Improving responses to cyber incidents	- An organised and unified response to future cyber incidents	- 'robust and effective structures to promote cybersecurity and to respond to cyber-attacks'

[64] CISA, 'Securing Federal Networks.'
[65] DHS, 'Critical Infrastructure and Resilience.'
[66] National Initiative for Cybersecurity Careers and Studies, 'Cybersecurity Workforce Development Toolkit.'

Shared Strategic Goals	US	EU
		- 'enhancing and strengthening their capability and preparedness to prevent, detect and respond to network and information security problems and incidents' - 'Strengthen its response to cyber attacks'
Cooperation and collaboration among stakeholders	- Collaborate with our inter-agency, industry and international partners to advance our mutual interests	- 'boost EU-level cooperation, knowledge and capacity' - 'foster cyber defence research and innovation cooperation' - 'help the EU retain and develop the cybersecurity technological and industrial capacities necessary to secure its Digital Single Market'

3.3. Proposal of joint strategic goals

Considering the identified *shared goals*, this paper translates them into *joint strategic goals* that can be used to describe specifically what the EU and US would work on together, as opposed to just focusing on achieving those goals internally themselves. The main focus is on identifying the shared goals that if worked on together would be beneficial for both and would help the EU and US achieve their internal goals. Where could the US and EU benefit if they worked together?

3.3.1. Assisting each other in improving resilience

The EU and US could work on improving resilience and cybersecurity together. Both focus internally on achieving resilience and cybersecurity. Several key EU documents, such as A Global Strategy for the European Union's Foreign and Security Policy and EU Cyber Security Strategies (2013 and 2017) recognise the importance of resilience, including in the international context. The US has included resilience in its past strategies but it was 'never embraced as the central goal of our strategy. It has always been an ill-defined and vague concept'[67]. This is changing as the Cyber Solarium Commission in its report released in March 2020, included a series of recommendations focused on resilience[68]defining resilience in the context of cybersecurity as 'the capacity to withstand and quickly recover from attacks'[69]. Policymakers have picked up on the concept for example has Senator Angus King (I-Maine) said the report can be summed up in four words — define, develop, defend and deter. 'I would simplify this further, as these four words can be condensed into one concept: digital resilience'[70]. Hence the momentum is there in the US and equally in the EU. In the EU the working definition is similar and has been gaining momentum in policy discussion[71]. Since resilience is built through both internal and

[67] Richard A. Clarke and Robert Knake, *The Fifth Domain* (New York: Penguin, 2019).
[68] Ray Rothrock, 'Cyberspace Solarium Commission Highlights the Importance of Digital Resilience,' *Morning Consult*, 17 March 2020, https://morningconsult.com/opinions/cyberspace-solarium-commission-highlights-the-importance-of-digital-resilience/.
[69] Mark Montgomery, John Costello and Robert Morgus, 'Promoting National Resilience,' Cyberspace Solarium Commission, 22 April 2020, https://www.solarium.gov/events/promoting-national-resilience.
[70] Rothrock, 'Cyberspace Solarium Commission Highlights the Importance of Digital Resilience.'
[71] Kate Saslow, 'Global Cyber Resilience: Thematic and Sectoral Approaches,' *EU Cyber Direct*. October 2019, https://eucyberdirect.eu/wp-content/uploads/2019/10/saslow_rif.pdf; European Commission, 'Cybersecurity,' Shaping Europe's digital future, 25 August 2020, https://ec.europa.eu/digital-single-market/en/cyber-security.

external initiatives, including through close cooperation with international partners[72][73], the US and the EU could focus in their cybersecurity partnership on building out their resilience efforts now. Working together with the aim to increase resilience and cybersecurity would mean that the EU and US can learn from their approaches on getting better at resilience and cybersecurity, fostering the exchange of expertise that could lead to innovation and competition. The EU and the US could with the use of instruments aim to increase the ability to effectively function through an impairment, to stay operational while minimising harm, reputational damage, and financial loss, and to recover quickly. Resiliency involves understanding risks, knowing where you fall short, addressing those gaps and reducing your risk potential[74]. The focus on resilience as a concept that highlights learning from an attack and response and becoming more resilient next time around, makes cooperation beneficial for both if learnings are actively shared and responses are reflected.

3.3.2. Achieving a common understanding of threats and vulnerabilities

The US and the EU should make a common understanding of threats and vulnerabilities their joint strategic goal. They have implemented similar activities in order to achieve this goal internally, recognising that different stakeholders need to have situational awareness in order to prevent and respond effectively together. The next logical step is to broaden those efforts across communities and stakeholders in the EU and the US. Threats and vulnerabilities do not know boundaries, and the two economies and societies rely on the same technologies. Already businesses have recognised that it is important to gather information on threats and vulnerabilities from across different channels and between various stakeholders from the EU and the US. Both sides need actionable intel (to not make the same mistakes), and need to use resources effectively (avoid double activity). Working together could, moreover, build a basis for more strategic political reaction, where a common understanding of threats is a prerequisite.

For policymakers to create policies that foster IT security and resilience, it is important to really understand the threats and vulnerabilities that IT infrastructures face. Explaining a crisis in a comprehensive way is a necessary first step to understanding its implications, as well as responding and reacting to it holistically. 'The World Economic Forum reports that the landscape of threat intelligence has historically been fragmented, with a high dependency on private-sector stakeholders and limited public-sector involvement. Increasing the outcome-oriented information-sharing to all stakeholders, and not limiting it within a single organisation, sector or even state, is one mechanism to improve communication and coordination to foster resilience, especially if this data-sharing is scalable and does not compromise sources or privacy.[75] A common understanding is important for certain stakeholders, but there are limits to achieving this. For example, computer emergency response teams (CERTs) who have already organised globally run into the hesitation of members of the management team that do not live the culture of information sharing like the tech community and therefore may decide that they will not pass on the information gathered by their own company's CERT. This can be problematic if an incident affects companies worldwide. CERTs cannot quickly connect and learn from others if key information is not passed on or does not reach them in time. Management might not like to share due to potential image problems. Too much information sharing is still voluntary. Hence, there is room to explore joint instruments to achieve a common understanding of threats and vulnerabilities and make this a strategic goal.

3.3.3. Improving cooperation mechanisms among a diverse set of stakeholders

The EU and the US have understood that for effective responses to malicious cyber-activities, different stakeholders need to work together. Therefore they have implemented instruments to do this. Some of the initiatives do affect stakeholders in both the EU and the US. Improving cooperation mechanisms

[72] European Commission, 'Joint Communication on "A Strategic Approach to Resilience in the EU's External Action",' 7 June 2017, https://ec.europa.eu/commission/presscorner/detail/en/MEMO_17_1555.
[73] Saslow, 'Global Cyber Resilience: Thematic and Sectoral Approaches.'
[74] Ray Rothrock, 'Cyberspace Solarium Commission Highlights the Importance of Digital Resilience.'
[75] Saslow, 'Global Cyber Resilience: Thematic and Sectoral Approaches.'

among a diverse set of stakeholders makes strategic sense, as learning about each other's processes and connecting stakeholders across the Atlantic that need to work together would improve their ability to prevent, mitigate and respond to cyber incidents. This needs to be facilitated and incentivised.

3.3.4. Improve cybersecurity workforce

Both the EU and the US emphasise workforce development by aiming to increase capacity, foster innovative research and stimulate education and skill development through different policies and funding. There is the benefit of working together on some aspects of workforce development more strategically to enable careers in cybersecurity and increase the number of people working in this field globally. This can ultimately lead to more resilience of third states, which in turn can mean more resilience in the EU and the US. Therefore, the paper identifies four main joint strategic goals that the EU and the US should concentrate on achieving together. Suitable joint instruments to achieve those goals will now be identified.

4. EU/US cybersecurity policies

To find out what instruments the EU and the US can do together in order to achieve joint goals, the paper first examines what instruments the EU institutions (the EU) and the US federal government (the US) have available to them by analysing how they conduct their cybersecurity policy. The focus here is on evaluating the different governmental resources that were used to implement those instruments. The results will show which instruments the EU and the US have in common but also which instruments may have certain limitations due to the way they are implemented.

4.1. How the EU conducts cybersecurity policy

The EU, a supranational organisation, has been active in conducting cybersecurity policy using a diverse set of instruments—a total of 35 were identified. The EU conducts cybersecurity policy in four key policy areas: security of the digital single market, cybercrime, common foreign and security policy and common security and defence policy. This section highlights some of the characteristics of how the EU conducts cybersecurity policy. The analysis will look at how the instruments are implemented, e.g. the EU can use regulations or directives to implement instruments or build its own capacity and resources. Another aspect is who they target, for example internal actors such as the member states, the private sector or academia and why the EU is introducing the instruments, e.g. the goals. Those aspects will give a bigger picture on how the EU conducts cybersecurity policy and whether it is similar to the US.

4.1.1. Directing: IT security and internal capacity building

The EU uses its legal and political authority[76] to implement some key instruments that aim to increase IT security and build capacity in the member states. Most of the instruments derive from the Directive on Security of Network and Information Systems (the NIS Directive), which is setting requirements for member states' legislatures to protect critical infrastructure. The NIS Directive 'foresees the attainment of a common high level of network and information security and thus upscaling capacities, cooperation and risk management practices across the EU Member States'.[77] Here the EU aims to achieve a certain outcome by directing (guiding) member states on what instruments need to be set in place in order to achieve the desired outcome. This is different from regulations, which are self-executing and do not require any implementing measures. Hence, without implementing the instruments on EU level, the EU still establishes instruments set in place on the member-state level to achieve EU cybersecurity policy goals such as the protection of critical infrastructure.

Cybersecurity instruments that the EU directed member states to implement are:

- Incident reporting—groups within the scope of the NIS Directive must notify a central authority of incidents that could significantly impact the continuity of services
- Have a point of contact on the member-state level for operational and technical response
- Set minimum standards
- Declare critical infrastructures for special protection
- Establish a national Computer Security Incident Response Team (CSIRT)

However, as well as making sure that certain instruments are implemented, a Directive can state in more detail what member states need to do in order to implement certain instruments successfully. A good example of such specification is the implementation of incident reporting for digital service providers (DSPs). Member States must ensure that DSPs notify the competent authority without undue delay of any cyber incident having a substantial impact on the provision of a service. NIS Directive Article 16

[76] See chapter method for definition.

[77] European Commission, 'State-of-Play of the Transposition of the NIS Directive,' 30 September 2020, https://ec.europa.eu/digital-single-market/en/state-play-transposition-nis-directive.

states that incident reporting is successful if it includes 'information to enable the competent authority or the CSIRT to determine the significance of any cross-border impact'.[78] Further in Article 16, some parameters are presented. Setting parameters is a way for the EU to have some influence on how incident reporting is specifically implemented by offering guidance.[79] Nevertheless, most details on implementation are decided on member-state level. This can lead to some divergences in use of instruments on the ground, as the EU directs the use of instruments[80] but EU institutions do not implement them themselves. As member states do the implementation, if not otherwise stated, intended outcomes such as information on incidents may not be accessible to the EU level unless member states pass them on voluntarily. Hence these are really instruments to increase capacity and IT security at member-state level and thereby increase the standard of IT security across the whole EU.

4.1.2. Framing and imposing costs: Harmonising principles and long-term goals in foreign, security and defence policy

Another way the EU conducts cybersecurity policy is by establishing frameworks as instruments to set principles and long-term goals. Four frameworks have been implemented in cybersecurity policy: (1) the certification framework, (2) the framework for screening of foreign direct investments, (3) the Permanent Structured Cooperation (PESCO) framework and (4) the framework for the joint EU diplomatic response to malicious cyber-activities 'cyber-diplomacy toolbox'. Those instruments form the basis of making rules and guidelines and direct the planning and development of implementation activities. All frameworks were passed by a regulation or, in case of PESCO, the Lisbon Treaty. This means that whatever is decided upon is binding. It must be applied in its entirety across the EU. What is being harmonised is agreed during the political process that leads to the regulation or treaty.

The certification framework enables the creation of tailored and risk-based EU certification schemes. This instrument is being implemented in the EU in order to enable certification of IT security of digital products, services and processes. The so-called certification schemes are defined by different stakeholders in the EU-level working group and then apply across the EU and are executed by agencies that are also defined in the regulation. This means that there cannot be any divergence among the member states and the EU defines the more normative aspects of the implementation as well, such as the 'who' and 'how'.

The framework for screening foreign direct investments is also passed by a regulation and offers a cooperation mechanism that ensures information sharing and analysis on the topic.[81] Here, in comparison to certifications that are new to many member states, it is harder to harmonise as member states have much more regulations of their own. Secondly, it is a foreign policy and national security topic, therefore the political process of harmonising is more difficult as member states have sovereignty in this field. So in the case of the framework of foreign investment screening, the EU as a supranational organisation uses the frameworks as an instrument that offers member states and EU institutions ways to work together on a long-term policy objective while still keeping their sovereignty as has been agreed through the political process. In practice this means that if, for example, Chinese companies invest in French cybersecurity companies that also sell components to German critical infrastructure providers, the framework would allow the German government to argue that this investment could become a

[78] European Union, 'Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 Concerning Measures for a High Common Level of Security of Network and Information Systems across the Union,' *Official Journal of the European Union*, 6 July 2016, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2016.194.01.0001.01.ENG.

[79] European Union Agency for Cybersecurity, 'Guidelines on Incident Notification for Digital Service Providers,' ENISA, 28 February 2017, https://www.enisa.europa.eu/news/enisa-news/guidelines-on-incident-notification-for-digital-service-providers.

[80] Bird&Bird, 'Developments on NIS Directive in EU Member States,' January 2020, https://www.twobirds.com/~/media/pdfs/developments-on-nis-directive-in-eu-member-states.pdf.

[81] European Commission, 'EU Foreign Investment Screening Regulation Enters into Force,' 10 April 2019, https://ec.europa.eu/commission/presscorner/detail/en/IP_19_2088.

European Order and Safety issue. Then the European Commission could look into the investment offer and make a recommendation to France: France would have to publicly reply to the recommendation but would not be required to follow it.

It is even more difficult to achieve long-term political goals in the policy area of defence, including cyber defence. The PESCO framework introduced by the Lisbon Treaty on European Union (articles 42.6, 46 and Protocol 10) can be seen as a first attempt to achieve harmonisation and work towards common goals in defence, which is in its entirety a member-state responsibility. PESCO is a framework and process to deepen defence cooperation between the EU Member States that are able and willing to do so. It is therefore an instrument supported on the EU level but implemented multilaterally by different member states. Hence neither of the projects is EU-wide. Projects that have emerged from this are nevertheless interesting as they can lead to further closer actions or be a test field. Outcomes of the framework so far are, for example, the offers of other instruments, such as penetration testing, joint capabilities development, and mutual operational support through the project 'Cyber Rapid Response Teams and Mutual Assistance in Cyber Security'. These are instruments the EU does not yet provide. The second project, under PESCO, where again not all member states are involved is the 'Cyber Threats and Incident Response Information Sharing Platform', which 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. Both PESCO projects focus on areas where inter-state coordination and the pooling of resources would increase state resilience to and crisis management of cyberattacks. Although each of these projects fall short of the EU-wide response, 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.[82]

The framework for a joint EU diplomatic response to malicious cyber-activities, the cyber-diplomacy toolbox, is another example where the EU uses a framework to achieve joint responses in an area that is governed by member states. This framework was passed by a Council Conclusion, which means that the Council has expressed a political position on this topic and has set up the framework as a political commitment but it is not legally binding. This is an important difference from frameworks that are introduced via a regulation that can make some aspects of the framework binding, as seen in the certification framework or the foreign investment screening framework. The cyber-diplomacy toolbox aims to enable the EU and its Member States to leverage the full continuum of EU policies and instruments, including if necessary restrictive measures, to keep cyberspace open, stable and secure. The cyber-diplomacy toolbox aims to achieve different goals of the EU in a global context, such as:

- Contributing to conflict prevention, mitigation of cybersecurity threats and greater stability in international relations
- Contributing to strengthening the rules-based order in cyberspace, including the application of international law and adherence to norms of responsible state behaviour
- Encouraging cooperation, facilitating mitigation of threats and influencing behaviour in the longer term

Within the framework, as in the others, there are different instruments that can be used. Instruments that are used are 'may be public or private, and may or may not be accompanied with coordinated attribution at EU level'.[83] Even though instruments become available through the toolbox, they can only be implemented with a unanimous decision by all member states. Hence political willingness and legal authority may limit the implementation of instruments. One example is the instrument of sanctions,

[82] PESCO Projects, 'Cyber Rapid Response Teams and Mutual Assistance in Cyber Security,' PESCO, https://pesco.europa.eu/project/cyber-rapid-response-teams-and-mutual-assistance-in-cyber-security/.

[83] European Union Agency for Cybersecurity, 'Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities: Cyber Diplomacy Toolbox,' ENISA, 2019, https://www.enisa.europa.eu/events/artificial-intelligence-an-opportunity-for-the-eu-cyber-crisis-management/workshop-presentations/20190603-eeas-eu-cyber-diplomacy-toolbox.pdf/view.

which was added to the toolbox. It was accompanied by a legal framework for sanctions against cyberattacks. The implementation of sanctions, however, now depends on the process and the support of member states.[84] Here the framework offers a path to use certain instruments on the EU level that member states individually might not apply. However, it poses some challenges: for example, if member states have not implemented sanctions in reaction to malicious activities, there is no practice in using them, and member states may have different views and need different information in order to support the implementation of an instrument such as sanctions. Hence, here the framework offers guidance and opportunities to work together on the topic where there is some political intention to respond on the EU level but the exact instruments are discussed on a case-by-case basis.[85] One instrument from the toolbox, public communications, has already been implemented, e.g. there was a statement in the Declaration by the High Representative of the Union for Foreign Affairs and Security Policy (HR/VP) on behalf of the EU condemning a cyberattack against Georgia.

Here the EU, instead of drawing from its internal resources and using them for external actions, applies more traditional non-cyber-specific instruments from foreign and security policy. These may include démarches, communications by the HR/VP, funding of capacity-building projects in third countries, or the issuing of general or specific Council conclusions on malicious cyber-activities in order to have a signalling function, set out action and underline awareness and determination of the EU and its member states to prevent and respond to potential attempts to weaken EU unity or positions of the EU and its Member States. Restrictive measures such as sanctions mostly need to be authorised and include instruments like travel bans, arms embargoes and freezing funds; they need unanimous decision. It may also support of lawful responses: 'In grave instances, malicious cyber activities could amount to a use of force or an armed attack within the meaning of the Charter of the United Nations. In this latter case, Member States may choose to exercise their inherent right of individual or collective self-defense as recognized in Article 51 of the Charter of the United Nations and in accordance with international law, including international humanitarian law. A Member State may also choose to invoke article 42 (7) TEU to call on other Member States to provide aid and assistance.'

For non-EU countries, like the US, EU Council decisions are important because they show the common political position within the EU and that follow-up political decisions may be taken at EU level on the topic, rather than just by member states individually.

Hence, the instruments used for external action are somewhat different and represent traditional foreign instruments. For example, the Council conclusions are an instrument to signal to external and internal actors when EU Heads of Member States have reached a common political decision on a specific issue, such as the 2020 Council conclusion condemning cyberattacks on Georgia. This not only signals the political position to external actors but also signals to EU institutions that further actions could be taken. For example, in theory this may mean that the EEAS follows up on the decision to condemn cyberattacks with a coordinated action that could lead to further information sharing or the use of other instruments available, such as sanctions, or member states take initiative to propose listing[86] that is then discussed in political dialogue followed by a legal assessment at EU level. Hence for non-EU countries, like the US, EU Council decisions are important because they show the common political position within the EU and that follow-up political decisions may be taken at EU level on the topic, rather than just by member states individually.

[84] Yuliya Miadzvetskaya, 'Challenges of the Cyber Sanctions Regime Under Common Foreign and Security Policy (CFSP),' *Security and Law*, vol. 7 (1 October 2019), http://dx.doi.org/10.2139/ssrn.3463153.

[85] Council of the European Union, 'EU Imposes the First Ever Sanctions Against Cyber-Attacks,' press release, 30 July 2020, https://www.consilium.europa.eu/en/press/press-releases/2020/07/30/eu-imposes-the-first-ever-sanctions-against-cyber-attacks/; German Federal Foreign Office, 'We Must Now Look to the Future' (interview by Foreign Minister Heiko Maas with Interfax), 11 August 2020, https://www.auswaertiges-amt.de/en/newsroom/news/maas-interfax/2374058

[86] German Federal Foreign Office, 'We Must Now Look to the Future.'

The instrument 'support of lawful response' has not been implemented yet, so it is more difficult to show how the implementation can look like. However, in theory it means that it was agreed upon on EU level that the EU can support lawful responses by member states in reaction to a cyber attack that would rise to the level of armed aggression. Hence the Cyber Diplomacy Toolbox states indirectly that member states can invoke the mutual defense clause[87] or the solidarity clause[88] and the EU can then assist with for example diplomatic steps or support individual and coordinated responses.

"

Frameworks in general are an indication that the EU works closely with member states on long-term goals and ultimately aims to harmonise the implementation of instruments as much as politically feasible.

All in all, frameworks in general are an indication that the EU works closely with member states on long-term goals and ultimately aims to harmonise the implementation of instruments as much as politically feasible. In policy fields, such as cyber defence, frameworks can be set up to show the intention of closer cooperation and allow a testing ground for new instruments that could become EU-wide instruments if politically feasible. Frameworks that are implemented through regulation instead of non-binding Council conclusions show more political will to harmonise, as they can make the implementation of instruments such as certifications mandatory. In policy areas such as EU cyber diplomacy as part of a common foreign and security policy and also in cyber defence, where member states have the sovereignty, instruments are made available to use on EU level. The frameworks aim to give guidance and offer constant political dialogue. Whereas the certifications framework is part of the EU digital single market, where the EU holds more legal and political power and none of the member states have on their own implemented the instrument yet, the framework is set to govern the path to harmonisation where at the end the consensus found, e.g. the certification schemes defined, will apply to every member state.

4.1.3. Shaping and promoting: International norms for responsible behaviour

The EU has been involved in the dialogue on international norms as an entity. It is consulted by the United Nations Group of Governmental Experts (GGE) on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security (formerly: on Developments in the Field of Information and Telecommunications in the Context of International Security), a UN-mandated working group in the field of information security.[89] The EU thus uses participation in those processes as an instrument to bring its viewpoint into the dialogue. Additionally, its response framework includes a broad array of potential reactions to negative cyber behavior. Here, as one EU cyber diplomat said, the EU would not always seek to 'impose costs' on norm breakers; rather the 'diplomatic toolkit' includes 'talks about normative behavior' with violators in the hope of changing minds'.[90] Such a diplomatic instrument can be for example a démarche that is sent to the norm violator. The EU adopted these so-

[87] 'This clause provides that if an EU country is the victim of armed aggression on its territory, the other EU countries have an obligation to aid and assist it by all the means in their power, in accordance with Article 51 of the United Nations Charter. This obligation of mutual defence is binding on all EU countries.' EUR-lex, 'Lex Access to European Union Law,' https://eur-lex.europa.eu/summary/glossary/mutual_defence.html.

[88] In June 2014, the European Union Council adopted a decision on the implementation of the 'solidarity clause' that obliges the Union and the member states to act jointly if a member state is the object of a terrorist attack or the victim of a natural or man-made disaster. Anna-Maria Osula, 'EU Solidarity Clause and 'Cyber Disaster,' CCDCOE, the NATO Cooperative Cyber Defence Centre of Excellence, https://ccdcoe.org/incyder-articles/eu-solidarity-clause-and-cyber-disaster/.

[89] United Nations, 'Regional Consultations Series of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security,' 2019. https://www.un.org/disarmament/wp-content/uploads/2019/12/collated-summaries-regional-gge-consultations-12-3-2019.pdf.

[90] Theresa Hitchens, 'US Urges "Like-Minded" Countries to Collaborate on Cyber Deterrence,' *Breaking Defense*, 24 April 2019, https://breakingdefense.com/2019/04/us-urging-likeminded-countries-to-collaborate-on-cyber-deterrence/.

called confidence-building measures to reduce the risks of conflict stemming from the use of information and communication technologies.[91]

4.1.4. Gathering and sharing: Common situational picture about threats and vulnerabilities

By gathering and sharing information on threats and vulnerabilities, the EU uses its strategic position of being in the centre and having access to a diverse set of stakeholders from the member states. This in theory allows EU institutions to see the whole picture on threats and vulnerabilities. Limitations may be access to information or its own capacity to retrieve information. Instruments that aim to achieve the goal of overview of the threat landscape or sharing information on vulnerabilities and how to deal with them are used by different actors. Here the EU is positioning itself as an information hub with the aim to achieve a common situational picture among different stakeholders within the EU to enable them, or to achieve joint responses, or to foster preventive measures and mitigation.

The EU is positioning itself as an information hub with the aim to achieve a common situational picture among different stakeholders within the EU to enable them, or to achieve joint responses, or to foster preventive measures and mitigation.

On a technical level, ENISA is dispersing guidelines, gathering and sharing best practices, and providing its own open-source threat information analysis.[92] For example, the EU may publish best practices on election security having consulted with all member states. Especially for member states that have limited resources to spend on gathering this information themselves, getting this information from the EU is an advantage. The EU also however relies on information being passed on by member states. To guarantee that this happens as much as possible, the EU resorts to two sets of instruments. The first set is aimed at building its own capacity. In order to respond to malicious cyber-activities, the EU created its own entities focused on the issue, namely EU-CERT and ENISA, or added personnel at EU INTCEN (EU Intelligence and Situation Centre—the intelligence hub). By building its own organisations, the EU aims to ensure that threat information specifically focused on its own institutions and incident response can be handled by EU-CERT. Other instruments that provide the necessary means for technical response may be passed on through networks built on EU level, e.g. the CSIRT network. This network was established under Article 12 of the NIS Directive with the aim to develop confidence and trust between the member states and to promote swift and effective operational cooperation. The aim of the network is to increase the information available to all; however, this is on a voluntary basis,[93] by promoting and funding the use of technical tools such as Malware Information Sharing Platform (MISP),[94] which allows for easier and standardised sharing of information.

[91] Organization for Security and Co-operation in Europe Permanent Council, '1092nd Plenary Meeting of the Council,' 10 March 2016, https://www.osce.org/pc/227791.

[92] European Union Agency for Cybersecurity, 'Threat Landscape,' ENISA, https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends.

[93] NIS Directive Article 12 b and c: 'at the request of a representative of a CSIRT from a Member State potentially affected by an incident, exchanging and discussing non-commercially sensitive information related to that incident and associated risks; however, any Member State's CSIRT may refuse to contribute to that discussion if there is a risk of prejudice to the investigation of the incident; and exchanging and making available on a voluntary basis non-confidential information concerning individual incidents'; EUR-Lex, 'Lex Access to European Union Law,' Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union,' EUR-Lex, 19 July 2016, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2016.194.01.0001.01.ENG.

[94] MISP, 'MISP – Open Source Threat Intelligence Platform & Open Standards For Threat Information Sharing,' https://www.misp-project.org/.

The second set of instruments focuses on the strategic response. To ensure information is being gathered or actions are taken that help identify the overall risks or threats, there are some instruments that incentivise those actions with political backing. An example is the threat reports that the Council can ask certain EU institutions[95] to give it. For assessing cyber threats these may rely on intelligence gathered from member states, or open source intelligence (OSINT) that is also provided by EU INTCEN and ENISA. In this case, the Council, which develops the common foreign and security policy of the EU and adopts international agreements,[96] has decided that more information on certain threats would be useful. With such political backing, it may be then easier for EU INTCEN to approach member states for classified information.

The EU acts as a provider, offering workshops, summits and platforms to meet and facilitating studies and educational campaigns that include a diverse set of stakeholders.

Another example, which shows what is possible if there is political backing to achieve a joint threat, risk or vulnerability analysis, is the EU-coordinated risk assessment on the 5G supply chain.[97] Information provided by member states allowed the collection of information on main assets, threats and vulnerabilities related to the 5G infrastructure and main risk scenarios in their countries. This coordinated risk assessment was done by member states following the Commission's Recommendation on the Cybersecurity of 5G Networks,[98] which was in response to the Council expressing its support for a concerted approach to the security of 5G networks.

This shows that the EU, even without using its legal power, has implemented instruments that led to joint actions at EU level to achieve better situational awareness on threats, vulnerabilities and risks.

4.1.5. Providing and innovating: Coordination and cooperation to get better at resilience and IT security

In order to achieve better EU-wide responses to become more resilient, the EU uses instruments that focus on bringing stakeholders together so they can share their experiences or develop actions jointly. Here the EU acts as a provider, offering workshops, summits and platforms to meet and facilitating studies and educational campaigns that include a diverse set of stakeholders. These instruments allow stakeholders from across the EU to work together on diverse cybersecurity (policy) issues. A very active forum working on IT security and resilience is the NIS Cooperation Group established by the NIS Directive, which functions according to the European Commission Implementing Decision of 1 February 2017 following its own rules of procedure.[99] 'A "decision" is binding on those to whom it is addressed (e.g. an EU country or an individual company) and is directly applicable.'[100] Hence the members of the

[95] In the Council Decision of 24 June 2014 for the arrangement for implementation of the solidarity clause, it was decided that in order to regularly assess the threats facing the Union, the European Council may request the Commission, the High Representative for Security Policy, and other Union agencies to produce reports on specific threats which can include cyber threats. CCDCOE, 'Council Decision of 24 June 2014 on the arrangements for the implementation by the Union of the solidarity clause,' *Official Journal of the European Union*, 1 July 2014, https://ccdcoe.org/uploads/2018/11/EU-140624-Solidarity.pdf.

[96] Council of the European Union, 'What does the Council of the EU do?', 17 July 2019, https://www.consilium.europa.eu/en/council-eu/.

[97] European Commission, 'Member States Publish a Report on EU Coordinated Risk Assessment of 5G Networks Security,' 9 October 2019, https://ec.europa.eu/commission/presscorner/detail/en/IP_19_6049.

[98] European Commission, 'Commission Recommendation (EU) 2019/534 of 26 March 2019: Cybersecurity of 5G Networks,' *Official Journal of the European Union*, 29 March 2019, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019H0534&from=GA

[99] EUR-lex, 'COMMISSION IMPLEMENTING DECISION (EU) 2017/179 of 1 February 2017 laying down procedural arrangements necessary for the functioning of the Cooperation Group pursuant to Article 11(5) of the Directive (EU) 2016/1148 of the European Parliament and of the Council concerning measures for a high common level of security of network and information systems across the Union,' *Official Journal of the European Union*, 2 February 2017, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32017D0179&from=EN.

[100] European Commission, 'Types of EU Law,' https://ec.europa.eu/info/law/law-making-process/types-eu-law_en

cooperation platform need to follow the rules and procedures, which makes actions more binding than loose voluntary cooperation mechanisms. The NIS cooperation group was implemented as a tool to cooperate, coordinate and thereby work on establishing a higher standard of IT security.[101] What this may look like offers an insight into the practice of what this group has produced. For example, after the coordinated risk assessment on 5G was published, the Cooperation Group was used as an instrument to gather and agree on a toolbox of mitigating measures to address the identified cybersecurity risks at national and EU levels,[102] which were then further discussed in the political process. Hence here the EU uses its own capacity and strategic position to gather stakeholders in a cooperation platform and thereby develop joint measures for IT security and resilience.

Example: Providing cooperation platforms to inform election security

The NIS Cooperation Group published a compendium on election security,[103] which shares experiences and provides guidance as well as an overview of tools, techniques and protocols to detect, prevent and mitigate such threats. Although the measures described in this are still voluntary, the cooperation platform offered the capacity for stakeholders to come together and share their best practices.

Example: Blueprint for incident response

The EU uses its strategic standing in order to create for itself and member states guidelines for cooperation and coordination in the blueprint for incident response in large-scale cyberattacks.[104] The blueprint was recommended by the European Commission and is therefore not legally binding, so the EU uses other instruments to induce stakeholders to use the described processes: exercises and trainings for EU institutions and the relevant stakeholders in member states to jointly practise responses. Moreover, the cooperation platforms already set up enable the EU to assist in a coordinated response. For example, in an incident at the technical level, the central mechanism for cooperation in the Blueprint is the CSIRT Network, chaired by the Presidency and with secretariat provided by ENISA, and, for the strategic and horizontal response, the Council Horizontal Working Party on Cyber Issues was established to ensure coordination in the Council and can be involved in both legislative and non-legislative activities.

Overall, these cooperation and coordination instruments are implemented to achieve IT security and resilience and are used by the EU as a strategic element to involve relevant stakeholders from across the member states. The EU in order to find vulnerabilities and threats and thereby improve cybersecurity of different stakeholders, uses also innovative instruments—specifically experimenting with activities that may be new and not used in other policy fields (yet). Hackathons, or bug bounty challenges are instruments used to identify and mitigate vulnerabilities and require unique technical skills. As well as regular cybersecurity exercises provide a more innovate way to tackle the challenges. Ultimately these cooperation mechanisms lead to the use of further instruments such as best practice sharing, joint risk assessment, exercises and guidelines.

[101] 'The Group's overall mission is to achieve a high common level of security of network and information systems in the European Union. It supports and facilitates the strategic cooperation and the exchange of information among EU Member States.' European Commission, 'NIS Cooperation Group,' 24 July 2020, https://ec.europa.eu/digital-single-market/en/nis-cooperation-group.

[102] European Commission, 'Secure 5G Networks: Questions and Answers on the EU Toolbox,' 24 July 2020, https://ec.europa.eu/commission/presscorner/detail/en/qanda_20_127.

[103] NIS Cooperation Group, 'Compendium on Cyber Security of Election Technology,' CG Publication 03/2018, July 2018, https://www.ria.ee/sites/default/files/content-editors/kuberturve/cyber_security_of_election_technology.pdf.

[104] European Commission, 'Annex to the Commission Recommendation on Coordinated Response to Large Scale Cybersecurity Incidents and Crises.'

4.1.6. Funding: Research, vulnerability research, innovation and capacity

To foster innovation, research and an increase in capacity among internal and external actors, the EU provides funding, which is supported by the the European Union Framework Programme for Research and Innovation 2021–2027 (Horizon Europe). This programme is informed by the Strategic Plan for Horizon Europe. Any cybersecurity-funded research therefore should drive the implementation of the relevant parts of Digital Europe and Horizon Europe programmes according to the multi-annual strategic plan. The 2019 document on the strategic plan for Horizon Europe mentions the goals of 'Increased cybersecurity based on more effective use of digital technologies, strong orientation on privacy and fundamental rights and a robust digital infrastructure to counter cyber-attacks'.

Another tool that guides EU funding is the four Horizon 2020 pilot projects, which will develop a sustainable European cybersecurity competence network.[105] This network is in line with the proposal for a regulation that would establish a European Cybersecurity Industrial, Technology and Research Competence Centre and a Network of National Cybersecurity Coordination Centres in 2021[106] and aims to pool Europe's cybersecurity expertise and prepare the European cybersecurity landscape. Previously funding was dispersed into four Horizon 2020 pilot projects (CONCORDIA, ECHO, SPARTA and CyberSec4Europe); in the future these will develop a sustainable European cybersecurity competence network. Thereby, the EU does not solely focus on research but also on funding innovation and capacity that emerges from the network's goals. 'The network should implement a variety of tasks such as cybersecurity demonstration cases in eHealth, finance, telecommunications, smart cities, transportation, Cyber Range, training or programmes to tackle the cybersecurity-skills gap in the EU and deliver innovative marketable solutions made in the EU to tackle the future cross domain cybersecurity challenges.'[107]

Overall, funding can be seen as another resource for the EU to support EU cybersecurity policy goals and/or achieve the implementation and use of certain instruments, such as training, sharing of information, development of best practices and guidelines or increasing awareness.

Overall, funding can be seen as another resource for the EU to support EU cybersecurity policy goals and/or achieve the implementation and use of certain instruments, such as training, sharing of information, development of best practices and guidelines or increasing awareness. For example, the EU has provided funding under the call 'Protecting the infrastructure of Europe and the people in the European smart cities of Horizon 2020'; the Commission allocated around €7–8 million per project to address both physical and cyber threats to critical infrastructure. The latest Connecting Europe Facility (CEF) cybersecurity call offers funding opportunities to key stakeholders identified by the NIS Directive such as European CSIRTs, operators of essential services (e.g. banks, hospitals, electricity and gas providers, railways, airlines, domain name providers) and various public authorities. Example projects funded are Secure and Safe Internet of Things (SerIoT) references—security frameworks and technological validation to optimise Internet of Things (IoT) platforms and networks information security in a holistic and cross-layered approach—and the EU provided grants to gather and benchmark, e.g. the SAINT (Systemic Analyser in Network Threats) project. Moreover, ENISA funds proactive detection of network security incidents and the EU supports the use and development of the MISP open source

[105] European Commission, 'Four EU Pilot Projects Launched to Prepare the European Cybersecurity Competence Network,' Shaping Europe's Digital Future, 3 October 2019, https://ec.europa.eu/digital-single-market/en/news/four-eu-pilot-projects-launched-prepare-european-cybersecurity-competence-network.

[106] European Commission, 'Proposal for a European Cybersecurity Competence Network and Centre,' Shaping Europe's Digital Future, 19 September 2018, https://ec.europa.eu/digital-single-market/en/proposal-european-cybersecurity-competence-network-and-centre.

[107] Cyber Competence Network, 'Four EU Pilot Projects to Prepare the European Cybersecurity Competence Network,' 2020, https://cybercompetencenetwork.eu/about/.

threat intelligence platform and open standards for threat information sharing. Hence by funding certain activities the EU can to some extent foster the implementation of its instruments.

In foreign policy, the EU has mostly focused on funding capacity building. In specific regions, the Commission has also used other instruments, including the European Neighbourhood Instrument (ENI) to help countries of the Eastern Partnership (Armenia, Azerbaijan, Belarus, Georgia, Moldova, Ukraine) to define strategic priorities related to the fight against cybercrime. The Instrument of Pre-accession (IPA) finances a new action of €5 million to help countries in South-Eastern Europe and Turkey to cooperate on cybercrime. The roll-out of more actions in these areas is foreseen in the coming years, also through other financing instruments. Innovation and research in cybersecurity was funded between the EU and Japan and was foreseen between the EU and the USA.

The difference with funding as a resource for cybersecurity policy aimed at external rather than internal actors is that in foreign policy, funding is less concentrated on the implementation of instruments such as best practice development, focusing more on creating research and cooperation as well as capacity building.

4.1.7. Summary

How the EU conducts cybersecurity policy tells a story about how the EU as a supranational organisation uses its governmental resources (treasury, political/legal authority, information and organisational capacities) to implement instruments and for what reasons. This can determine to what extent instruments are used, where they are implemented and whether the implementation is mandatory or non-binding. The EU directed member states to ensure a minimum layer of protection for critical infrastructure, which is an internal security issue. Here the EU politically agreed on the implementation of certain instruments at a member-state level, which means that details of the implementation may differ across the EU because they are decided at that level. The EU uses frameworks in foreign and security policy as well as in policy areas where the goal is that implementation of instruments should be harmonised in the long run. Here instruments are defined but their implementation may still differ across the EU. The EU also uses its strategic position to share and gather information and thereby implement instruments that aim to achieve a better situational picture and increase resilience and awareness. It can do this to a greater extent if it increases its own organisational capacities, but may be limited by them, in which case it relies on member states' capacities. Here the EU applies instruments that incentivise information sharing on the EU level, e.g. possibility of threat reports. Providing these coordination and cooperation mechanisms and creating guidelines for joint responses is another way the EU aims to ensure the implementation of instruments. The EU thus is on the one hand focusing on building capacity and on the other incentivising the use of its instruments to become more resilient together. Last but not least important, the EU uses funding as a resource to push the implementation of instruments such as capacity building, developing best practices and research.

All in all, it is important to understand the EU's resources and their limitations, as they explain the implementation of instruments. In certain sub-policy areas within the EU's cybersecurity policy, such as foreign and security policy or cyber defence, policy implementation is less convergent across member states or instruments are not implemented on the EU level (yet), as the EU has less political and legal authority in those fields. In those areas the EU provides information and organisational resources for cooperation and coordination or frames the political discourse of instruments. In areas where there is more political backing by member states, the EU harmonises the instruments by making certain details binding for stakeholders. Instruments are also used again and again in different fields and are implemented by different resources.

The next section answers the same questions for the US and thereby identifies the extent to which the EU as a supranational organisation and the US federal government are similar in the way they conduct cybersecurity policy.

4.2. How the US federal institutions conduct cybersecurity policy

The US federal institutions ('the US' below) have been active in conducting cybersecurity policy using a diverse set of instruments defined as governmental interventions to achieve policy objectives: a total of 58 have been identified. These instruments are used as a response to malicious cyber-activities. The US conducts cybersecurity policy in key policy areas: national security, defence policy, cyber crime, foreign policy and economy policy. This section will highlight some of the characteristics of how the US conducts cybersecurity policy. The analysis will also look at how the instruments are implemented, for example through congressional decision regulating the implementation of certain instruments (e.g. standards) or the use of its own organisational capacity to implement instruments (e.g. draft guidelines). Another aspect is who the instruments are targeted at: for example, internal actors such as the federal agencies themselves, the private sector or academia. Finally, the reasons why US federal institutions are implementing the instruments, e.g. the goals they aim to achieve, are examined. These aspects give a bigger picture of how the US federal level conducts cybersecurity policy, and allow comparisons with the EU.

4.2.1. Directing: Regulation of its federal agencies

While cybersecurity of the private sector is regulated mostly through state legislatures and not on the federal level, this does not apply to US executive institutions. The legislative branch has made the implementation of some instruments mandatory for US federal agencies by passing regulations that define what the executive branch is required to do. These are aimed at enhancing its cybersecurity and enabling a better understanding of how to shape cybersecurity policy.

Box 1. Examples of instruments aimed at federal institutions passed by regulations

- To keep check of the money spent on cybersecurity specifically, the Consolidated Appropriations Act 2017 requires that a cybersecurity analysis is incorporated in the President's budget which aims to allow for further analysis over the years on the spending in this specific policy field
- The 2014 FISMA law requires federal agencies to develop, document and implement information security programmes and have independent evaluations done. For example, the Treasury has its own IT security programme with minimum standards.
- Federal agencies that are assigned a critical infrastructure and therefore have become a sector-specific agency are required to report regularly on critical infrastructure to the DHS.
- Federal agencies are expected to identify all positions that perform information technology cybersecurity due to the Federal Cybersecurity Workforce Assessment Act from 2017. For example, the Department of Defense (DoD) had to submit to the congressional committees a report on the feasibility of an apprentice programme to support job training.
- The Trump Administration issued an Executive Order (EO) addressing cybersecurity, 'Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure' (11 May 2017). It directs federal executive agency heads to undertake various cybersecurity-related reviews and to report findings back to the White House within prescribed timetables ranging from 60 days to one year.

Hence the US on a federal level is targeting its own federal institutions with regulations on how to achieve IT security and with instruments that aim to assist in developing cybersecurity policy.

4.2.2. Innovating: Finding vulnerabilities and talent with technical instruments

In order to find vulnerabilities and threats and thereby improve cybersecurity of federal agencies and other stakeholders, the US uses innovative instruments—specifically experimenting with activities that may be new and not used in other policy fields (yet). Hackathons, competitions, bug bounty challenges and red teaming are instruments used to identify and mitigate vulnerabilities[108] and require unique technical skills. By implementing these activities, the US government can access expertise outside the government and promote careers in the field.[109] The instruments are mostly implemented by federal agencies using their own funding, capacity and informational resources to run them. For example, the DoD invited hackers to test enterprise system security used for global operations, and the Hack the Pentagon programme was the first bug bounty programme in the history of the federal government in 2016. DoD launched its Vulnerability Disclosure Policy, which provides a legal avenue for security researchers to find and disclose vulnerabilities in any DoD public-facing systems. 'The Hack the Pentagon programme has since enabled DoD to identify and remedy thousands of security vulnerabilities'[110] according to a press statement in 2018.

A technical programme that was more focused on highlighting talent was introduced by an EO in 2019,[111] the President's Cup Cybersecurity Competition. The programme, implemented by CISA, gave individuals and teams ten challenges to solve over an eight-hour period, testing various technical and security skills.[112]

These instruments have also been used to incentivise change of behaviour. The DHS offers red teaming and pen testing as activities to test cybersecurity of events or critical infrastructure networks. Red teaming can be used to test an organisation's security policy and make recommendations for improvements. In practice, the DHS's 90-day assessments begin with about two weeks of reconnaissance that might culminate in a carefully crafted spear-phishing email. 'We send a phishing email and it beacons back to our host in Arlington, and then we have a foothold' into the organisation, said Rob Karas, DHS's director of national cybersecurity assessments and technical services. 'From there, we pivot to other computers, to domain controllers, to enterprise computers.'[113] The DHS has carried out quiet 'red-teaming' exercises at three federal agencies, breaking into networks and telling agency officials how it was done.

Overall, the US uses those technical activities just like any other instruments to achieve its specific cybersecurity policy goals.

4.2.3. Framing: Standards, taxonomy and best practices

In order to manage cyber risks and improve cyber resilience or achieve the common use of a taxonomy across a diverse set of stakeholders, such as local agencies, local governments and critical infrastructure providers, the NIST has developed different frameworks. "Generally speaking, NIST guidance provides the set of standards for recommended security controls for information systems at federal agencies.

---

[108] The Department of Defense Strategy 2018 noted that the DoD will continue to identify crowdsourcing opportunities, such as hackathons and bug bounties, in order to identify and mitigate vulnerabilities more effectively and to foster innovation. US Department of Defense, 'Summary of the 2018 National Defense Strategy of the United States of America,' 2018, https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf.

[109] White House, 'President Donald J. Trump Is Strengthening America's Cybersecurity Workforce to Secure Our Nation and Promote Prosperity,' 2 May 2019, https://www.whitehouse.gov/briefings-statements/president-donald-j-trump-strengthening-americas-cybersecurity-workforce-secure-nation-promote-prosperity/.

[110] US Department of Defense, 'Department of Defense Expands "Hack the Pentagon" Crowdsourced Digital Defense Program,' 24 October 2018, https://www.defense.gov/Newsroom/Releases/Release/Article/1671231/department-of-defense-expands-hack-the-pentagon-crowdsourced-digital-defense-pr/.

[111] White House, 'Executive Order on America's Cybersecurity Workforce,' 2 May 2019, https://www.whitehouse.gov/presidential-actions/executive-order-americas-cybersecurity-workforce/.

[112] 'CISA Hosts First Annual President's Cup Cybersecurity Competition,' *Security Magazine*, 23 December 2019, https://www.securitymagazine.com/articles/91459-cisa-hosts-first-annual-presidents-cup-cybersecurity-competition.

[113] Sean Lyngaas, 'Red-Teaming by DHS "Quietly and Slowly" Uncovers Agency Vulnerabilities,' *CyberScoop*, 13 June 2018, https://www.cyberscoop.com/red-teaming-dhs-quietly-slowly-uncovers-agency-vulnerabilities/.

These standards are endorsed by the government, and companies comply with NIST standards because they encompass security best practices controls across a range of industries – an example of a widely adopted NIST standard is the NIST Cybersecurity Framework."[114] The implementation of instruments is therefore encouraged as "in many cases, complying with NIST guidelines and recommendations will help federal agencies and organisations ensure compliance with other regulations"[115]. Hence compliance has been broad even though it is voluntary. The US also actively supports the use of the frameworks by external actors by providing workshops, translations and giving talks about it.

Box 2. Most notable frameworks that introduce different instruments

- The National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework (NICE Framework), published in NIST Special Publication 800-181, is a blueprint to categorise, organise and describe cybersecurity work in Categories, Specialty Areas, Work Roles Tasks, and Knowledge, Skills and Abilities (KSAs). It aims to ensure a common taxonomy to describe cybersecurity work and workers regardless of where, or for whom, the work is performed. Internal actors can check their workforce using this framework and assess whether they lack any skills.
- NIST is a federal agency: part of the Department of Commerce. The NIST Framework is a somewhat living document and service; it has been translated to many languages and is used by the governments of Japan and Israel, among others. NIST worked with private-sector and government experts to create the framework, which was released in early 2014. The effort went so well that Congress ratified it as a NIST responsibility in the Cybersecurity Enhancement Act of 2014. In 2017 a draft version, version 1.1, was circulated for public comment. The framework helps organisations understand not only their cybersecurity risks (threats, vulnerabilities and impacts), but how to reduce these risks with customised measures. Version 1.1 is compatible with version 1.0. The changes include instruments such as guidance on how to perform self-assessments, additional detail on supply chain risk management and guidance on how to interact with supply chain stakeholders; a vulnerability disclosure process is encouraged.

The implementation can be voluntary or legally binding, depending on how the framework is passed. The NIST framework, for example, is voluntary, but NIST's compliance standards guide federal agencies and contractors to meet requirements mandated under FISMA and other regulations e.g.. Sarbanes-Oxley (SOX) and Health Insurance Portability and Accountability Act (HIPAA) or Defense Federal Acquisition Regulation Supplement (DFARS).

Hence the US federal institutions use frameworks to achieve higher resilience of different stakeholders and a common use of taxonomies. Even though they are initially voluntary, it has been found that their compliance assists federal agencies to meet standards set in regulations, e.g. FISMA, which was discussed under 'directing', and this may have an effect also on organisations that work with federal agencies and must fulfill those standards if compliance is written in the contract.

4.2.4. Providing: Coordination, cooperation and services to get better at resilience and cybersecurity

The US government provides different forms of cooperation mechanisms and services in order to foster resilience and cybersecurity. CISA offers services for internal actors that are available at no cost to federal agencies, state and local governments, critical infrastructure and private organisations. Examples are vulnerability scanning, risk assessment and phishing campaign assessments. The US provides services for assessing the cybersecurity level and making recommendations after the tests. CISA would offer scanning of Internet-accessible systems for known vulnerabilities on a continual basis. As potential

[114] Maureen Data Systems (MDS), 'National Institute of Standards and Technology (NIST),' https://www.mdsny.com/nist/.
[115] Nate Lord, 'What is NIST Compliance?,' *Digital Guardian*, 7 September 2018, https://digitalguardian.com/blog/what-nist-compliance.

vulnerabilities are identified, CISA notifies the organisation so that preemptive risk mitigation efforts may be implemented in order to avert vulnerability exploitation. Another service is the National Initiative for Cybersecurity Careers and Studies (NICCS), an online resource for cybersecurity training that connects government employees, students, educators and industry with cybersecurity training providers throughout the nation. The 'Department of Homeland Security Cyber Hunt and Incident Response Teams Act of 2019'—bipartisan legislation—directs the DHS to maintain permanent 'cyber hunt and incident response teams' to assist both government and private entities in their efforts to prevent and, when necessary, appropriately respond to cybersecurity attacks. A CSIRT is a concrete organisational entity (i.e. one or more staff) that is assigned the responsibility for coordinating and supporting the response to a computer security event or incident. US federal agencies provide many similar services to improve the level of cybersecurity of stakeholders.

The US provides its stakeholders with platforms to cooperate and coordinate. The software component transparency initiative is run by the National Telecommunications and Information Administration (NTIA), an agency of the Department of Commerce. This initiative is convening a multi-stakeholder process to develop greater transparency of software components for better security across the digital ecosystem. NTIA offers a platform to develop and execute an approach for how manufacturers and vendors can communicate useful and actionable information 'about the third-party/embedded software components that comprise modern software and IoT devices, and how this data can be used by enterprises to foster better security decisions and practices'.[116]

In order to respond to malicious activity effectively, US federal agencies have set up coordination platforms. These can be ad-hoc groups such as the Cyber Unified Coordination Group, which assembles during a significant incident, but also guidelines such as the National Cyber Incident Response Plan (NCIRP), which reflects and incorporates lessons learned from exercises, real-world incidents and policy and statutory updates, such as the Presidential Policy Directive/PPD-41: U.S. Cyber Incident Coordination and the National Cybersecurity Protection Act of 2014.

4.2.5. Funding: Research and innovation

Another way the US conducts cybersecurity policy is through funding research and technical innovation. How the US funds cybersecurity was elucidated by the Cybersecurity Enhancement Act of 2014, which requires the National Science and Technology Council (NSTC) and the Networking and Information Technology Research and Development (NITRD) Program to develop a strategy for cybersecurity research and development (R&D) to guide the overall direction of federally funded R&D in cybersecurity. The 2019 plan identifies four interrelated defensive capabilities (deter, protect, detect and respond) and six priority areas (artificial intelligence, quantum information science, trustworthy distributed digital infrastructure, privacy, secure hardware and software, and education and workforce development) for cybersecurity R&D. Section 630 of the Consolidated Appropriations Act, 2017 (Pub. L. No. 115-31) requires that a cybersecurity funding analysis be incorporated into the President's Budget. This is one way to find out how the US funds cybersecurity efforts. For example, the financial year (FY) 2019 President's Budget includes $15 billion of budget authority for cybersecurity-related activities, a $583.4 million (4.1%) increase on the FY 2018 estimate.[117] The budget shows how the US uses funding to foster research and innovation. For example, the US Department of Transportation, National Highway Traffic Safety Administration granted a study that gathered best practices and observations in the field of cybersecurity involving electronic control systems across a variety of industry segments where safety of life is concerned. When the US funds cybersecurity technologies, it aims to help move these technologies into broader use. To achieve this, the DHS's Transition to Practice (TTP) programme was set up.

[116] National Telecommunications and Information Administration, 'NTIA Software Component Transparency,' 7 July 2020, https://www.ntia.doc.gov/SoftwareTransparency.

[117] White House, 'Cybersecurity Funding,' 2018, https://www.whitehouse.gov/wp-content/uploads/2018/02/ap_21_cyber_security-fy2019.pdf

Additionally, Congress may pass funding for a specific effort, such as the allocation of about $425 million in funding for election security ahead of the 2020 presidential election in 2019. Hence the US uses funding to foster research and innovation and the use of state-of-the-art security hardware and software.

4.2.6. Gathering and sharing: Common situational picture of threats and vulnerabilities

In order to achieve a common situational picture, the US uses instruments such as guidelines on how to gather and share classified and open-source information with internal and external stakeholders, instruments to encourage the sharing of information, such as the establishment of analysis centres, tools to analyse the information such as political threat reports, and tools that lead to the spread of information, such as alerts.

Instruments that aim to encourage the sharing of information on threats and vulnerabilities were introduced. Here it is important to differentiate between instruments that encourage the gathering and sharing of such information within the private sector and between private sector and governmental agencies.

Box 3.

Instruments that aim to encourage information sharing within the private sector

- Information Sharing Analysis Centers were introduced and promulgated pursuant to Presidential Decision Directive-63 (PDD-63) signed on 22 May 1998, after which the federal government asked each critical infrastructure sector to establish sector-specific organisations to share information about threats and vulnerabilities.
- A funded award, the 'Neighborhood Keeper' programme for good threat detection and shared threat intelligence across small infrastructure providers is supported by the Department of Energy (DoE).

Instruments that aim to increase the sharing of information by the government with the private sector or by the private sector with the government

- The DHS's National Network of Fusion Centers provide information sharing and analysis for an entire state. These centers, run by state and local governments, are designed to take what may seem to be disparate pieces of information on a variety of subjects and 'fuse' them in order to be able to recognise threat indicators. An example of a fusion centre that focuses on cyber matters is the DC NTIC (National Capital Region Threat Intelligence Consortium) Cyber Center.
- The Cybersecurity Information Sharing Act of 2015 directed the Director of National Intelligence, the Secretary of Homeland Security, the Secretary of Defense and the Attorney General, in consultation with the heads of the appropriate federal entities, to jointly develop and issue procedures to facilitate and promote e.g. timely sharing of classified cyber-threat indicators (CTIs) and defensive measures (DMs) in the possession of the federal government with representatives of relevant federal entities and non-federal entities that have appropriate security clearances; timely sharing with relevant federal entities and non-federal entities of CTIs, DMs, and information relating to cybersecurity threats or authorised uses under this title in the possession of the federal government that may be declassified and shared at an unclassified level; and timely sharing with relevant federal entities and non-federal entities, or the public if appropriate, of unclassified, including controlled unclassified, CTIs and DMs in the possession of the federal government.
- The vision of the Enhance Shared Situational Awareness (ESSA) Initiative is to create real-time cybersecurity situational awareness, to enable integrated operational actions, and to improve the security of the US government and US critical infrastructure. ESSA lays the foundation to share the right information, in time to make a difference and in formats that reduce human workload and time to action.

- The DHS's free Automated Indicator Sharing (AIS), which participants connect to a DHS-managed system in the DHS's National Cybersecurity and Communications Integration Center (NCCIC) that allows bidirectional sharing of CTIs.
- In April 2017, the Intelligence Community Security Coordination Center (IC SCC) deployed a capability—the Intelligence Community Analysis and Signature Tool (ICOAST)—to increase sharing of cybersecurity threat intelligence at the top-secret security level.
- The National Security Agency (NSA) receives and disseminates information relevant to cybersecurity at the top-secret, secret and unclassified levels.
- The Cyber Information Sharing and Collaboration Program (CISCP) enables information exchange and the establishment of a community of trust between the federal government and critical infrastructure owners and operators.
- State, Local, Tribal and Territorial (SLTT) regulators may have mandatory reporting requirements for certain types of cyber incidents in certain sectors. Incident reporting is therefore encouraged by provisions of platforms and networks. However, there may be mandatory reporting on incidents such as the DoD Reporting Requirements on Cyber Breaches and Loss of PII and CUI. In the case of 'a significant loss of personally identifiable information [PII] [or] controlled unclassified information [CUI] by a cleared defense contractor', the Secretary 'shall promptly submit to the congressional defense committees notice in writing of such loss'. Whether or how this provision will impact notification requirements for contractors and vendors remains to be seen.
- The US-CERT Incident Reporting System provides a secure web-enabled means of reporting computer security incidents to US-CERT.
- The DoD Reporting requirements for cleared defence contractors.
- The National Cybersecurity Center within the DHS coordinates and integrates information from six centres to provide cross-domain situational awareness, analysing and reporting on the state of US networks and systems, and fostering inter-agency collaboration and coordination.

Instruments that aim to foster the sharing of information with external stakeholders

- Agreement between the US and Europol and Supplemental Agreement between Europol and the US on the Exchange of Personal Data and Related Information.
- Classified information sharing is governed by the provision of guidelines. US federal agencies share intelligence about malicious cyber-activities with certain partner countries. The 'Five Eyes' intelligence alliance of five English-speaking nations has joined forces with Japan, Germany and France to introduce an information-sharing framework on cyberattacks from countries such as China, people linked to the Japanese government have said[118].

Political and technical threat and vulnerability assessment is aiming to follow up the gathering and sharing efforts and to lead to concrete steps that can be political or technical.

[118] Mainichi Japan, 'Five Eyes Intel Group Ties Up with Japan, Germany, France to Counter China in Cyberspace,' *The Mainichi*, 4 February 2019, https://mainichi.jp/english/articles/20190204/p2a/00m/0na/001000c.

Box 4. Instruments that support the assessment of threats and vulnerabilities

- Presidential Policy Directive–Critical Infrastructure Security and Resilience Presidential Policy Directive/PPD-21 and EO 13636 demand that sector-specific agencies must support the Secretary of Homeland Security's statutory reporting requirements by providing, on an annual basis, sector-specific critical infrastructure information.
- Federal agencies assess threats and vulnerabilities; determine deviations from acceptable configurations, enterprise or local policy; assess the level of risk; and develop and/or recommend appropriate mitigation countermeasures in operational and non-operational situations.
- Technical report on the Cyber Threat and Vulnerability Analysis of the US Electric Sector by US DoE Office of Scientific and Technical Information.
- The DHS's Continuous Diagnostics and Mitigation programme built a dashboard, the CDM, which provides agencies with overall data on their cybersecurity risks and vulnerabilities.
- The US intelligence community presents assessment of threats to US national security to members of the US Senate Select Committee on Intelligence (sometimes referred to as the Intelligence Committee or SSCI), which is dedicated to overseeing the US intelligence community. The statements reflect the collective insights of the intelligence community.
- A 'statement for the record' worldwide threat assessment of the US intelligence community presented in Congress and published. It includes a section on cyber-activities.

Finally, the US implements instruments that are specifically aimed at alerting stakeholders in urgent cases.

Box 5. Instruments that aim to alert and increase the awareness of specific target audiences in order to implement protection measures

- An ICS-CERT Alert is intended to provide timely notification to critical infrastructure owners and operators concerning threats or activity with the potential to impact critical infrastructure computing networks.
- National Security Agency (NSA) cybersecurity advisory: patch remote desktop services on legacy versions of Windows.
- Joint US–UK technical alert on malicious cyber-activity carried out by the Russian government.

For the US, public attribution of cyberattacks to state and non-state actors is seen as an instrument that includes the process by which evidence of a malicious cyber-activity is collected, analysed and associated to an originating party (the attacker). Public attribution is used to alert internal actors such as companies about ongoing malicious activities. These alerts usually are accompanied by necessary information to identify the actors and deploy defences. An example is a joint NSA and Federal Bureau of Investigation (FBI) report that looks at Russian malware and gives clear advice on defence measures that can be taken.[119] This form of public attribution with technical alerts is also done jointly with other countries, as the 2018 US–UK joint technical alert about malicious cyber activity carried out by the Russian government, by the (UK) National Cyber Security Centre (NCSC), the FBI and the DHS, shows.[120]

[119] National Security Agency and Federal Bureau of Investigation, *Russian GRU 85th GTsSS Deploys Previously Undisclosed Drovorub Malware*, August 2020, https://media.defense.gov/2020/aug/13/2002476465/-1/-1/0/csa_drovorub_russian_gru_malware_aug_2020.pdf

[120] National Cyber Security Centre, 'Joint US–UK Statement on Malicious Cyber Activity Carried out by Russian Government,' 15 April 2018, https://www.ncsc.gov.uk/news/joint-us-uk-statement-malicious-cyber-activity-carried-out-russian-government.

That those attribution efforts are directed at internal actors also became clear during the public attribution of the WannaCry ransomware that was directed at companies within the US by calling on 'the private sector to increase its accountability in the cyber realm by taking actions that deny North Korea and the bad actors the ability to launch reckless and disruptive cyber acts'.[121]

Overall, the US has invested many different instruments to achieve a situational picture as well as to increase awareness about threats and vulnerabilities that may foster better preparedness.

4.2.7. Shaping and promoting: International norms for responsible behaviour, application of international law

The US federal government shapes the application of international law and the development of international norms for responsible behaviour by using instruments such as participation in international groups and through statements on how the law and norms apply. In 2011, the White House issued the International Strategy for Cyberspace, which noted that 'The development of norms for state conduct in cyberspace does not require a reinvention of customary international law, nor does it render existing international norms obsolete. Long-standing international norms guiding state behavior—in times of peace and conflict—also apply in cyberspace.' However, the strategy said that 'unique attributes of networked technology require additional work to clarify how these norms apply and what additional understandings might be necessary to supplement them'. Cyberspace opens up novel and extremely difficult legal issues with which lawyers grapple.[122]

The Tallinn Manual from 2012 is an academic, non-binding study on how international law applies in cyberspace. The Tallinn Manual 2.0 was developed[123] in 2019. The US government shapes the application through communication of its own position. In a speech on 18 September 2012, State Department Legal Adviser Harold Koh explained the US position on how international law applies to cyberspace asking 'How do we apply old laws of war to new cyber-circumstances, staying faithful to enduring principles, while accounting for changing times and technologies?'.[124] An analysis by Michael N. Schmitt (Chairman and Professor, Department of Law, United States Naval War College) in *Harvard Law Review* shortly after shows the convergences in position of the US government represented by Koh's speech and the Tallinn Manual, which was published three weeks before the speech. Schmitt concluded that the Tallinn Manual and the speech 'are but initial forays into the demanding process of exploring how the extant norms of international law will apply in cyberspace'[125]. Hence communication about its viewpoint is one instrument to shape the discussions on the application of international law.

Another instrument the US used to shape international norms was its participation in the UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (UNGGE). In the DoD Strategy 2018, the US government reinforces the norms that were agreed upon by saying that: "the United States has endorsed the work done by the UNGGE to develop a framework of responsible State behavior in cyberspace. The principles developed by the UNGGE include prohibitions against damaging civilian critical infrastructure during peacetime

[121] White House, 'Press Briefing on the Attribution of the WannaCry Malware Attack to North Korea,' 19 December 2017, https://www.whitehouse.gov/briefings-statements/press-briefing-on-the-attribution-of-the-wannacry-malware-attack-to-north-korea-121917/.

[122] Quote from Harold Hongju Koh, Legal Adviser, US Department of State: 'I find more and more of my time is spent grappling with the question of how international law applies in Cyberspace.' Harold Hongju Koh, 'International Law in Cyberspace,' *Harvard International Law Journal*, vol. 54 (December 2012), https://digitalcommons.law.yale.edu/cgi/viewcontent.cgi?article=5858&context=fss_papers

[123] National Security Archive, 'Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations,' 24 April 2019, https://nsarchive.gwu.edu/news/cyber-vault/2019-04-24/tallinn-manual-20-international-law-applicable-cyber-operations.

[124] 'Since the speech had been fully cleared in the interagency process, it can be viewed as reflecting the U.S. Government's views on the issues, not just those of Mr. Koh or the State Department.' Michael N. Schmitt. 'International Law in Cyberspace: The Koh Speech and Tallinn Manual Juxtaposed,' *Harvard International Law Journal*, vol. 54 (December, 2012), https://harvardilj.org/wp-content/uploads/sites/15/2012/12/HILJ-Online_54_Schmitt.pdf.

[125] Michael N. Schmitt, 'International Law in Cyberspace: The Koh Speech and Tallinn Manual Juxtaposed.'

and against allowing national territory to be used for intentionally wrongful cyber activity. The Department will work alongside its interagency and international partners to promote international commitments regarding behavior in cyberspace.[126] Hence the US is promoting and shaping international norms in cyberspace.

4.2.8. Imposing costs: Public attribution, indictments, extradition, sanctions, ban of products, and other instruments of national power

The US has taken steps to punish malicious behaviour and infraction of the norms of behaviour. It has started to use legal and economic instruments to do so as well as aiming to build an alliance of partners to use these means together: the Cyber Deterrence Initiative. This is intended to impose costs and thereby deter future malicious activities by state and non-state actors.[127] One instrument to do this is extradition: the process to deliver a person accused or convicted of committing a crime in another jurisdiction to US law enforcement. It is a cooperative law enforcement process between the two jurisdictions and depends on the arrangements made between them. An example is the case of a 20-year-old wanted for hacking offences in the US who was set to be the first Cypriot citizen to be extradited. The US also asked to extradite Laurie Love, a British citizen, but a British appeals court rejected this, citing the inability of US prisons to humanely and adequately treat his physical and mental ailments.

Another legal tool the US uses is indictments: a criminal accusation that a person has committed a crime. On 19 May 2014, the Department of Justice indicted five Chinese military hackers for computer hacking and economic espionage directed at six entities in the US nuclear power, metals and solar products industries. The US has charged four members of China's People's Liberation Army for hacking into the credit-reporting agency Equifax.

Box 6. The role of attribution in punishing state or non-state actors

Public attribution of cyberattacks to state and non-state actors is the process by which evidence of a malicious cyber-activity is collected, analysed and associated to an originating party (the attacker). This attribution does not necessarily have to be public but the US has publicly attributed cyberattacks. When directed at external actors, attribution is the instrument to use in order to justify follow-up actions. Hence attribution in this regard is not solely an instrument in itself but is used in combination with other instruments. Examples are the public attribution to Chinese hackers that led to the No-Spy Agreement and an attribution to the Russian government followed up with indictments and expelling diplomats.

A more economically focused legal instrument is the cyber-related sanctions programme, which represents the implementation of multiple legal authorities. Some of these authorities are in the form of executive orders issued by the President. Other authorities are public laws (statutes) passed by Congress. These authorities are further codified by the Department of the Treasury's Office of Foreign Assets Control (OFAC) in its regulations, which are published in the Code of Federal Regulations (CFR). OFAC announced sanctions targeting three state-sponsored cyber groups responsible for North Korea's malicious cyber-activity on critical infrastructure.

[126] US Department of Defense, 'Summary Department of Defense Cyber Strategy 2018,' September 2018, https://media.defense.gov/2018/sep/18/2002041658/-1/-1/1/cyber_strategy_summary_final.pdf.
[127] White House, 'National Cyber Strategy.'

Box 7. All instruments of national power

The John S. McCain National Defense Authorization Act really shaped the US position on what constitutes the imposition of consequences, making instruments in cyberspace and other domains available and noting that all instruments of national power can be used in response to certain states: 'The Russian Federation, People's Republic of China, Democratic People's Republic of Korea, and the Islamic Republic of Iran in cyberspace (e.g., zero-day discovery, tool-development, and preposition of malware) and through other instruments of national power'.

4.2.9. Competing: Monitoring, counterintelligence, offensive cyber operations

The US identifies countries that pose risks to US cybersecurity as an instrument to enable responses that aim to 'disrupt, defeat and deter cyber attacks'. Those countries and actors are clearly communicated in advance; for example, in the National Cyber Strategy 2018 the countries identified are Iran, China, North Korea and Russia.

Persistent engagement and its instruments

In 2018, significant changes in US strategic guidance were made as the National Security Strategy, National Defense Strategy and DoD Cyber Strategy were adapted to a new approach: strategic competition. These developments support the view that a central challenge for the US lies in strategic competition in cyberspace that doesn't rise to the level of armed conflict and that deterrence strategy on its own is not an effective anchoring approach for ensuring security in this strategic competitive space. In response to the new means of influence and coercion allowing US adversaries to increasingly exploit cyberspace below the threshold of armed conflict, the new approach aims to achieve superiority in cyberspace.

Persistent engagement was best described by Anne Neuberger, the senior NSA official who leads the NSA Cybersecurity Directorate: 'Knowing that we're not waiting for the incident, we're tracking, we're understanding, we're degrading their capabilities, their ability to operate in a way that hopefully prevents that key attack.'[128] In order to do this, the US uses its monitoring techniques to enable the detection and localisation of threats together with counterintelligence and offensive cyber operations to track and counter foreign operations. The head of the NSA, Paul Nakasone, argues that 'persistent presence is what the Intelligence Community is able to provide us to better understand and track our adversaries in cyberspace'[129].

The instruments to enable 'persistent engagement' are spread across agencies and are closely intertwined. There is an evolving role of US Cyber Command, and its new posture of 'persistent engagement' using a 'cyber-persistent force'. Nakasone notes that: "We must 'defend forward' in cyberspace, as we do in the physical domains. Our naval forces do not defend by staying in port, and our airpower does not remain at airfields. They patrol the seas and skies to ensure they are positioned to defend our country before our borders are crossed. The same logic applies in cyberspace. Persistent engagement of our adversaries in cyberspace cannot be successful if our actions are limited to DOD networks. To defend critical military and national interests, our forces must operate against our enemies on their virtual territory as well. Shifting from a response outlook to a persistence force that defends forward moves our cyber capabilities out of their virtual garrisons, adopting a posture that matches the cyberspace operational environment."[130]

[128] Greg Myre, '"Persistent Engagement": The Phrase Driving a More Assertive U.S. Spy Agency,' *NPR*, 26 August 2019, https://www.npr.org/2019/08/26/747248636/persistent-engagement-the-phrase-driving-a-more-assertive-u-s-spy-agency?t=1600432098051.

[129] Gen. Joseph F. Dunford Jr, 'Defending Forward,' *Joint Force Quarterly*, vol. 92 (1st Quarter 2019), USMC, https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-92/jfq-92.pdf.

[130] Paul M. Nakasone, 'A Cyber Force for Persistent Operations,' *Joint Force Quarterly*, vol. 92 (February 2019), https://www.459arw.afrc.af.mil/News/Article-Display/Article/1737519/a-cyber-force-for-persistent-operations/.

Interagency missions

Cyber Command works in concert with other domestic agencies, each doing its part towards the overarching goals and assisting other departments' missions with its activities.[131] In the Cybersecurity Strategy 2018, the DoD's role was changed to become an enabler, so for example its resources can be used to work together with the DHS to ensure critical infrastructure protection. Around 50 military personnel at DHS are funded by DoD to work at CISA, which is responsible for protecting the nation's critical infrastructure from physical and cyber threats. Monitoring techniques in order to detect and localise threats is done mostly by the DHS. CISA's NCCIC provides 24/7 cyber situational awareness through for example monitoring, threat analysis, incident response and cyber defence. Its monitoring activities focus on domestic networks and federal networks, while Cyber Command and NSA use offensive cyber operations and counterintelligence to gather information in external networks.

According to Nakasone: "In persistent engagement, we enable other interagency partners. Whether it's the FBI or DHS, we enable them with information or intelligence to share with elements of the CIKR [critical infrastructure and key resources] or with select private-sector companies. The recent midterm elections is an example of how we enabled our partners. As part of the Russia Small Group, USCYBERCOM and the National Security Agency enabled the FBI and DHS to prevent interference and influence operations aimed at our political processes. Enabling our partners is two-thirds of persistent engagement. The other third rests with our ability to act—that is, how we act against our adversaries in cyberspace. Acting includes defending forward."[132] Hence the US competes in cyberspace using instruments such as monitoring and counterintelligence as well as instruments that allow for interagency missions, such as personnel exchanges.

4.2.10. Managing: Vulnerabilities disclosure and management

Another way the US conducts cybersecurity policy is by implementing instruments that aim to manage vulnerabilities. The US has defined a coordinated vulnerability disclosure (CVD) process that aims to reduce the adversary advantage while an information security vulnerability is being mitigated. CISA's CVD programme coordinates the remediation and public disclosure of newly identified vulnerabilities in products or services. The US also implemented a vulnerability equity process (VEP) that is used by the federal government to determine on a case-by-case basis how it should treat zero-day vulnerabilities (the ones that are not known to the vendor): whether to disclose them to the public to help improve general computer security or use them offensively.

4.2.11. Summary

How the US conducts cybersecurity policy tells a story about how and why the US federal government uses its resources (treasury, political/legal authority, information and organisational capacities) to implement instruments. This can determine to what extent instruments are used, where they are implemented and if the implementation is mandatory or non-binding.

To achieve internal cybersecurity policy goals, such as better IT security, resilience and situational awareness, the US passes regulations that target federal institutions and make certain IT-security standards mandatory, whereas to target the private sector, the US is framing–not regulating—standards. Other ways the US conducts cybersecurity policy are by implementing instruments that aim to manage vulnerabilities (managing instruments aim to achieve the responsible disclosure of vulnerabilities to vendors) and through funding research and technical innovation. A big part on how the US conducts cybersecurity policy is by providing services and cooperation platforms. Here the US is innovating by including technical instruments to achieve IT-security; for example, the DHS offers red teaming and penetration testing as activities to test cybersecurity of event infrastructures, critical infrastructure

[131] Brig. Gen. Timothy D. Haugh, Eighth Annual International Conference on Cyber Engagement (ICCE), 23 April 2019, https://www.youtube.com/watch?v=PjBqSWZbLtM.
[132] Dunford, 'Defending Forward.'

networks and so on. Those instruments have also been used to incentivise change of behaviour towards better IT-security implementation without necessarily regulating.

Most instruments are implemented through gathering and sharing in order to achieve a situational picture as well as increase awareness about threats and vulnerabilities that may foster better preparedness among various domestic stakeholders. This has been accompanied by setting up of coordination and cooperation platforms, including guidelines that reflect and incorporate lessons learned from exercises, real-world incidents and policy and statutory updates, with the aim that every stakeholder knows their part.

In terms of cybersecurity policy at the intersection of national security, foreign policy and economic policy, the US firstly identifies countries that pose risks to US cybersecurity as an instrument to enable responses that aim to 'disrupt, defeat and deter cyber attacks'. Here the US is taking different approaches: competing, punishing, and promoting and shaping international norms. Especially with countries identified as a risk, the US competes and persistently engages with them in cyberspace using instruments such as monitoring, offensive cyber operation and counterintelligence as well as instruments that allow for interagency missions, such as personnel exchanges to ensure the interplay of instruments that are available to the different agencies. The US has taken steps to punish and thereby aim to deter malicious behaviour. It has started to use a number of legal and economic instruments to do so as well as aiming to build an alliance of partners to use those means together, the Cyber Deterrence Initiative.

Finally, the US has supported the international norms and is working alongside its inter-agency and international partners to promote international commitments.

5. Identifying the commonalities

Overall, the US and the EU have 32 instruments[133] in common that are implemented to achieve their cybersecurity policy objectives. These include the use of public statements when condemning malicious activity, cyber dialogues in cyber diplomacy, operational agreement to achieve technical information sharing and the requirement to have a contact point for responses at different agencies. Other instruments that focus on achieving a higher cybersecurity level of stakeholders are also similar, e.g. providing national and international exercises, competitions and training of responses, provision of guidelines/frameworks for standardisation and taxonomy, and early warning/public vulnerability or (attributed) threat alerts.

In the way that they conduct cybersecurity policy, the EU and the US also have some commonalities. Both direct certain actors to meet expectations, such as the use of standards, using their legal and political authority to do so, even though they may differ in what actors they target and what rules they set. Directing for both is a way of ensuring that certain instruments are implemented. Both use framing to achieve long-term harmonisation and guide the use of instruments by stakeholders. The US and EU both provide resources to stakeholders, although those resources may differ. Both use gathering and sharing techniques for situational awareness; there is quite some overlap in how this is done. Both fund cybersecurity research and innovation. Finally, both shape and promote international norms in cyberspace.

[133] The annex lists all instruments in more detail, with examples of implementation, and gives a clearer comparative picture of the resources through which instruments are implemented.

How the EU conducts cybersecurity policy

How the US conducts cybersecurity policy

In conclusion, the EU and US conduct cybersecurity policy in similar ways and use similar instruments to achieve strategic objectives. This means that there is potential in diving deeper into what future cooperation can look like. In order to identify which instruments the EU and US can implement together, the paper analyses the instruments that they have already implemented together to gain a better understanding of what has been feasible to do together.

6. Past instruments implemented together

Looking at past instruments implemented together gives an indication of what may be feasible in the future. Here we also consider how this is done and what governmental resources are spent.

Of the 32 instruments the EU and the US have in common, they have jointly implemented only eight together so far. Some of the joint activities focused on providing capacity and setting up cooperation mechanisms that could lead to further collaboration. The two main ones are the cyber dialogue and the EU and US working group on cybersecurity and cybercrime that was established in the context of the 2010 Lisbon EU–US Summit. The working group has the clear mission to focus on the joint goals of countering global cybersecurity threats, cyber-incident management, public–private partnerships on critical infrastructure, awareness raising and cybercrime.

Specific actions that were taken together on those topics are as follows.

- Exercises: The US–EU working group on cybersecurity and cybercrime did a transatlantic cyber exercise and organised information exchanges on national and regional cyber exercises
- Personnel exchanges by FBI and Europol
- Operational agreements to work together and exchange of technical information that includes forensic police methods and investigative procedures between Europol and the US
- Digital forensic capabilities
- The gathering and sharing of best practices, e.g. in fora such as the Global Forum for Cyber Expertise and in EU–US dialogues

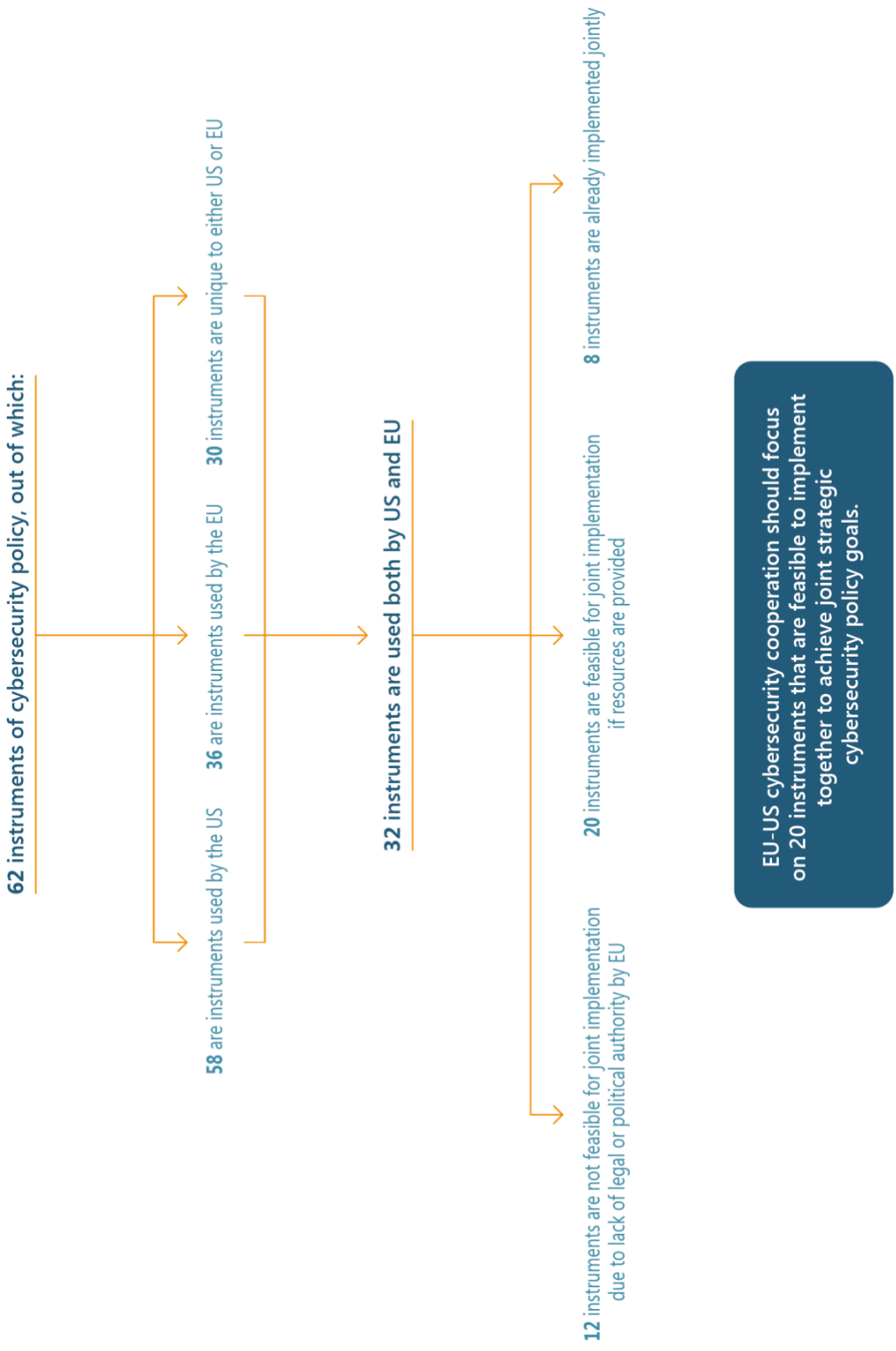
- Multi-stakeholder consultations (EU–US): Call for proposals for regulatory cooperation activities to inform the Executive Working Group (EWG) to consider reducing unnecessary administrative obstacles and costs, while at least preserving the level of protection of each side in terms of cybersecurity
- The joint promotion of national cyber awareness month
- Capacity building in third countries, e.g. Georgia, Ukraine

The main joint activities so far have concentrated on setting up cooperation mechanisms and gathering and sharing information for increased joint situational awareness as well as the promotion and use of tools to do this. The EU and US use instruments that they already internally apply, and just apply them together. Some of these activities are happening only once, such as the exercises or the awareness-raising activities; others are regular established formats, like the personnel exchanges, the working group, the cyber dialogue and the sharing of technical information supported by an agreement. The sharing of information and the personnel exchanges are the only two instruments that were implemented through legal authority. Those actions show that joint implementation was supported by a clear strategic goal developed in a working group with regular exchange and contact points.

Looking at the eight instruments implemented together, there are three prerequisites for joint implementation of instruments:

- The need for specific joint strategic goals
- The need for cooperation mechanisms supported by regular exchange
- The need for own capacity and availability to contribute to the joint endeavour

Keeping these in mind, the paper will look at what limitations may exist and may hinder the joint implementation of instruments. The paper considers whether those limitations could be overcome in the short term to implement an activity together or whether addressing the limitation would take longer and therefore instruments with high limitations should be excluded from further analysis. For that, the paper identifies the most important limitations and evaluates whether they will have a strong impact on implementation feasibility in the next one or two years or whether they can be overcome easily.


62 instruments of cybersecurity policy, out of which:
58 are instruments used by the US
36 are instruments used by the EU
30 instruments are unique to either US or EU
32 instruments are used both by US and EU
12 instruments are not feasible for joint implementation due to lack of legal or political authority by EU
20 instruments are feasible for joint implementation if resources are provided
8 instruments are already implemented jointly
EU-US cybersecurity cooperation should focus on 20 instruments that are feasible to implement together to achieve joint strategic cybersecurity policy goals.

7. Accounting for limitations for joint implementations of instruments

Looking at limitations for joint implementation gives context on how feasible it is to implement instruments together. This is not to say that instruments with limitations can never be done together: instead, the policymakers' focus would be on addressing the limitations first in order for the instrument to become available for joint implementation. Until then, only the instruments which limitations are low are considered further.

7.1. Availability of instruments

The first limitation is the availability of instruments. As the paper defines joint responses as actions taken together, it is less about coordinating different actions and focuses more on actions that the EU and the US implement jointly. A limitation therefore could be if either side has not previously implemented this action alone. A prerequisite for a joint activity is that the instruments are actually available on both sides. When looking at what has already been done together, all the activities in some shape or form are implemented externally or internally beforehand in the context of cybersecurity policy. This underlines that it is not feasible to propose instruments that are not available on either side for a joint action in the near future. Hence any instrument that is not available on either side highly limits the implementation of a joint action as a response to malicious cyber-activities. It could be overcome by implementing the instruments at an EU level first: discussions with the US about joint implementation could follow. It is unlikely that the EU would implement an instrument with the US before implementing it internally first.

The limitation 'availability of instrument' eliminates 30 instruments from being considered for joint implementation, as this limitation is hard to overcome in the short term. Instruments that are therefore excluded for joint implementation are red teaming, military network defensive capabilities, military offensive capabilities, CVD processes, vulnerability equity management processes and technical services, e.g. vulnerability scanning.

7.2. Lack of capability

Another limitation is lack of capability, which is the power or ability to do something. This affects mostly instruments that rely on technical skills but also instruments that rely on strategic leadership. For the technical part, capability models can be an indicator by which individuals and organisations obtain, improve and retain the skills, knowledge, tools, equipment and other resources needed to do their jobs competently. On a technical level, these can be analysed by using the NIST cybersecurity framework (CSF), the NIS Directive or the cybersecurity capability maturity model (C2M2): just three of several models to choose from, each providing a comprehensive approach that can be used to measure the maturity of cybersecurity capabilities. In defence and security, capabilities are referred to as defence technology and equipment (also as 'capability').[134] The analysis applied here takes account of capability as a governmental resource that is given when a governmental entity can use its own capacity to build capabilities such as risk assessments.[135]

In the EU, some capabilities are found at a member-state level, not directly on the EU level. This is because for the most part 'the aim is to bring cybersecurity capabilities at the same level of development in all the EU Member States and ensure that exchanges of information and cooperation are efficient, including at cross-border level'.[136] In defence, the focus is also on the development and pooling of capabilities, where the EU provides the framework or funding for this rather than developing its own

[134] European Commission, 'The European Defence Fund: Questions and Answers,' 7 June 2017, https://ec.europa.eu/commission/presscorner/detail/en/memo_17_1476.

[135] Tagged in annex with organisational power.

[136] European Commission, 'EU Cybersecurity Initiatives,' January 2017, https://ec.europa.eu/information_society/newsroom/image/document/2017-3/factsheet_cybersecurity_update_january_2017_41543.pdf.

capabilities.[137] Hence capabilities are a limitation if the implementation of an instrument would rely heavily on capabilities found at member-state rather than EU level. It is of course a possibility, but would require the joint work of member states and would end up looking more like a coalition of the willing and *capable* rather than a joint EU–US activity as the paper seeks to identify. Moreover, past joint activities showed that the EU and the US both have the capabilities already. This limitation is considered high, but could be overcome if the EU institutions would build their own capabilities first.

The limitation 'lack of capability' eliminates one instrument for joint implementation which is the gathering and sharing of classified intelligence for which the EU level relies on member states capabilities.[138] EU INTCEN has mostly open-source analytical competencies but relies on member states to share their own classified intelligence. Open-source information sharing is further considered as a possible instrument for joint implementation.

7.3. Lack of legal or political authority

Another limitation is the lack of legal and political authority necessary to implement an instrument. A longer political or legal process could make it infeasible for the EU and US to implement an instrument together as they lack the legal or political authority that makes implementation possible. In the EU context this would mean all instruments where the EU does not have the competences or only shared competences with member states, and therefore might be reliant on approval by member states. The EU's competences are set out in the EU Treaties, which provide the basis for any actions the EU institutions take. The EU can only act within the limits of the competences conferred on it by the Treaties, and where the Treaties do not confer competences on the EU they remain with the member states [Article 5(2) TEU]. In certain areas, for example CFSP, the EU and member states have created the option to use certain instruments together, such as sanctions against cyber operations; however, implementation relies on unanimous approval by all member states. This is an internal process whereby the EU institutions facilitate the discussion but simply lack the legal and political authority for implementation: a joint implementation with the US could be limited by that. The US federal government has its own legal and political limitations and may be restricted by state power. Examples include the setting of standards or implementation of security programmes that are voluntary. Hence, taking account of the political and legal authority of the EU and US is important as this can highly affect the feasibility of joint implementation of instruments.

This limitation can be overcome, for example, for the joint use of foreign instruments such as sanctions on a case-by-case basis and through diplomatic dialogue. Other instruments may become available after extensive political dialogue and with the arrangement of legal agreements that give the EU level the authority to work together with the US, as was the case with the agreement between the US and the European Policy Office: it states in Article 3 that Europol and the US agree to exchange technical information including, but not limited to, forensic police methods and investigative procedures. Those processes take time and therefore this limitation is considered high, as this paper aims to identify joint activities to be implemented as soon as possible.

The limitation 'lack of political/legal authority' eliminates 12 instruments from joint implementation. It includes for example many foreign instruments such as sanctions, public attribution and démarches, but also internal instruments that are passed through legal actions, such as incident reporting requirements or declaration of what constitutes a critical infrastructure.

[137] European Commission, 'The European Defence Fund: Questions and Answers,' 7 June 2017, https://ec.europa.eu/commission/presscorner/detail/en/memo_17_1476.

[138] Gustav Gressel, 'Protecting Europe Against Hybrid Threats,' European Council on Foreign Relations, 25 June 2019, https://www.ecfr.eu/publications/summary/protecting_europe_against_hybrid_threats.

7.4. Resources (money, personnel)

For most instruments to be implemented, e.g. red teaming, exercises, cybersecurity research funding, audits and risk assessments, the EU and the US rely on significant amounts of resources. Depending on how the instrument is implemented, this may mean money, e.g. a funded research project, or people, who can be either their own human resources or the capacity of other stakeholders that are responsible for the implementation, e.g. implementing the risk assessments, creating exercises and training. Hence a joint implementation is limited to the extent that it would have to make resources available or use the ones already in place. A shortage of resources can affect the successful joint implementation of instruments set in place when the instrument is available but cannot be properly executed. Examples of this can be found in the EU and in the US. In the US, for example, the success of red teaming as a means to identify vulnerabilities proactively and close them is threatened because the demand exceeds the resources (trained personnel).

Box 8. Further reading on resources as a limitation in the US

- In Pomerleau, Mark, The Pentagon is handling cyber vulnerabilities inconsistently, The Fifth Domain, March 17th 2020, https://www.fifthdomain.com/dod/2020/03/17/the-pentagon-is-handling-cyber-vulnerabilities-inconsistently/: Pomerleau explains that due to resource limitations, red teaming cannot be effectively applied at the DoD: 'Without an enterprise wide solution to staff, train and develop tools for DoD Cyber Red Teams and prioritise their missions, DoD Cyber Red Teams have not met current mission requests and will not meet future requests because of the increased demands for DoD Cyber Red Team services'.
- In CyberSeek, Cybersecurity Supply/Demand Heat Map, https://www.cyberseek.org/heatmap.html, 2020, an initiative funded by the National Initiative for Cybersecurity Education (NICE), one can see a granular snapshot of demand and supply data for cybersecurity jobs at the state and metro area levels. This can be used to grasp the challenges and opportunities for cybersecurity workforce. The US had total cybersecurity job openings of 507,924 as of 2nd of October 2020.

Further reading on resources as a limitation in the EU

- In European Court of Auditors, Challenges to effective EU cybersecurity policy, 2019, https://www.eca.europa.eu/Lists/ECADocuments/BRP_CYBERSECURITY/BRP_CYBERSECURITY_EN.pdf it is argued that "as there is no dedicated EU budget to fund the cybersecurity strategy, there is not a clear picture of what money goes where. The three core bodies at the heart of the EU's cybersecurity policy – ENISA, Europol's EC3, and CERT-EU are facing resourcing challenges at a time of heightened security-driven political priorities. The current allocation of human and financial resources in the EU agencies remains a challenge for them to meet expectations".

The limitation 'lack of resources' could affect 20 instruments for joint implementation, such as funding to improve cybersecurity, cyber-threat and vulnerability (indicator) analysis, gathering and sharing of best practices, open-source cyber-threat intelligence gathering and sharing by government with other stakeholders or political/strategic threat assessment. However, a possible lack of resources can be addressed by EU-level institutions themselves and further analysis may show that there is potential even to save some resources through joint implementation, as efforts do not have to be doubled.

Box 9. Further reading on resources as a limitation in the US

For a joint activity the limitations of resources need to be accounted for, as both parties would have to make the needed resources available for a successful implementation. Therefore, when finding activities to do jointly, the following questions are important.

> Would a joint activity decrease or increase the resources that are available for implementation of the instrument?

Here, think long term or short term. Two examples: Comparing risk assessment approaches may mean an increase in resources in the short term as it is an extra task; however, if it is done with the goal to harmonise approaches or build a practical tool, it could lower the needed resources in the long term. Equally, a jointly funded research project may lower the investments for both sides.

> How feasible is it to make resources available for joint activities? Are these newly created resources or can current resources implement joint activities?

These questions ask whether new resources have to be created, or if current resources can simply manage the additional joint activity or resources can be shifted to implement the activity. Examples include the joint analysis of threats and whether there is already a person who has analysed threats for one side and could without much increase of workload share information on analysis with the counterpart. If such a person does not yet exist or the workload is already too high, a new person would have to be hired or the success of the joint activity might suffer due to the lack of capacity.

Looking at limitations identified the instruments that are more feasible than others to be implemented jointly in the near future. Any instruments that are available to only one side or where the EU lacks capability or political/legal authority cannot easily be implemented jointly.

If those limitations are addressed, then the instruments may become available for joint implementation in the future. However, until then, only the instruments for which limitations are low are considered further: for example, a lack of resources (money and personnel) that can after cost–benefit analysis be accounted for in the short term.

There is potential for the EU and the US to save resources by jointly implementing a certain instrument; for example, both countries do open-source analysis of threats and vulnerabilities that target companies which operate in the European market as well as the US market. The same information may be shared through different channels. Here the paper proposes to at least further analyse whether resources could be used more effectively if efforts are combined. Hence, going forward, the 20 instruments that have lower limitations for implementations are considered for possible joint implementation.

8. Recommendations: joint instruments accomplish joint strategic goals

Finally, the paper presents the possible joint response. A joint response is an action that the US and the EU take together in order to reach a joint strategic goal addressing malicious cyber-activity.

The paper identified 20 common instruments that are feasible to do together and have potential in addressing the joint strategic goals. The following seven recommendations describe how the 20 instruments could be implemented jointly in such a way that they help in accomplishing the joint strategic goals for responding to malicious cyber-activities.

Box 10. Instruments the EU and US have in common and that are feasible to do together to reach joint strategic goals

> Early warning/public vulnerability or (attributed) threat alerts

> Cyber-threat and vulnerability (indicator) analysis

> Open-source cyber-threat intelligence gathering and sharing by government with other stakeholders

> Technical response teams

- Awareness activities
- Funding to improve cybersecurity
- Gathering and sharing of best practices
- Multi-stakeholder consultations
- Cyber dialogue
- Political/strategic threat assessment
- Personnel exchanges, e.g. cyber liaison officer
- Accountability and evaluation of instruments
- Crisis response plan
- National and international exercises, competitions and training of responses
- Crowd-sourced vulnerability identification via hackathons and bug bounty challenges (with awards)
- Capacity building in third countries
- Specific topical (cooperation) working groups
- Cybersecurity research and development
- Provision of guidelines/frameworks for standardisation and taxonomy
- Digital forensics capacities

Recommendation 1: Develop joint technical bulletins

Develop and publish joint bulletins with technical analysis on malicious activities. A joint bulletin is a report-like publication (public, semi-public or confidential) that includes technical and optionally political analysis on a threat or an incident and is the result of analytic efforts between agencies. A secret bulletin to specific audiences may be accompanied by a public statement.

Instruments the recommendation draws upon:

- Early warning/public vulnerability or (attributed) threat alerts
- Cyber-threat and vulnerability (indicator) analysis
- Open-source cyber-threat intelligence gathering and sharing by government with other stakeholders
- Technical response teams
- Awareness activities

Joint strategic goals to be addressed:

- Assisting each other in improving resilience
- Common understanding of threats + vulnerabilities

Prevent malicious activity becoming successful and thereby increase IT security and the adoption of available prevention and mitigation instruments. The purpose of these bulletins is mainly to inform network device vendors, Internet service providers, public-sector organisations, private-sector corporations, and small offices/home offices (SOHOs) whose systems are affected, so they take steps.

For the EU and US the benefit of developing joint bulletin/alerts could be that the gathering of information and technical details if done jointly is more holistic and leads to a common technical understanding of threats and vulnerabilities affecting, for example, common critical infrastructure systems that are used in the EU and the US. The dissemination of a clear message to stakeholders that are the target audience for the EU and the US together could have the added benefit of ensuring that the target audience do not drown in an overload of information from many different sources.

Main features: Such bulletins draw on reported information, as well as information derived from industry sources and their own analysis. They give details on the systems affected, who the targets are and what the goals of the malicious activities are, as well as tactics, techniques and procedures (TTPs). They may contain indicators of compromise that will enable public- and private-sector critical infrastructure partners to take action to mitigate adverse impacts from this activity and protect their sensitive information: such information could be Internet protocol addresses, domain names, and malware indicators associated with malicious data exfiltration activity.

Use cases: Continuous malicious activities that affect critical infrastructure in the EU and the US, where prevention mechanisms are available and need to be implemented by stakeholders. Example: Joint Technical Alert by UK and US in 2018—'Advisory: Russian State-Sponsored Cyber Actors Targeting Network Infrastructure Devices'.[139] The US has used such bulletins to inform certain stakeholders via secure channels about ongoing malicious cyber-activity against US government and private-sector entities.[140]

Recommendation 2: Fund a process to develop joint automatic, standardised open source threat and vulnerabilities intelligence sharing solution among like-minded countries

The EU and the US should fund a process to develop a joint automatic, standardised threat intelligence-sharing solution. The end solution should provide incident responders and defenders in key critical infrastructures as well as companies that operate in the European and the US market with threat and vulnerability intelligence in an effective and efficient way.

Instruments the recommendation draws upon:

- Funding to improve cybersecurity
- Gathering and sharing of best practices
- Cybersecurity R&D
- Specific topical (cooperation) working groups
- Multi-stakeholder consultations
- Digital forensics capacities
- Provision of guidelines/frameworks for standardisation and taxonomy

Joint strategic goals to be addressed:

[139] National Cyber Security Centre,, 'Russian State-Sponsored Cyber Actors Targeting Network Infrastructure Devices,' 15 April 2018, https://www.ncsc.gov.uk/news/russian-state-sponsored-cyber-actors-targeting-network-infrastructure-devices.

[140] Cybersecurity and Infrastructure Security Agency (CISA), 'Update: Ongoing Malicious Cyber Activity Against U.S. Government and Private Sector Entities,' 1 March 2013, https://us-cert.cisa.gov/ncas/current-activity/2013/02/22/Ongoing-Malicious-Cyber-Activity-Against-US-Government-and-Private.

- Common understanding of threats and vulnerabilities
- Assisting each other in improving resilience
- Improving response mechanisms and cooperation among a diverse set of stakeholders

The EU's aim is to build resilience and IT security globally. One of the main elements to achieve this is cross-border collaboration. In particular, communication, information-sharing and coordination around cyber incidents is fundamental to resilience in cyberspace'[141]. If key players share information on threats, vulnerabilities, attacks, etc. then the entire ecosystem can adapt, creating a more resilient IT infrastructure. Most of the groundwork to achieve this—e.g. setting in place preventative measures, studying new threat actors and their emerging tactics and techniques, assessing vulnerabilities and mitigation of successful cyber incidents and learning from them—is being done by the global tech community, and in particular the CERT community, since 1990 with the establishment of the global Forum of Incident Response and Security Teams. Although policymakers and diplomats are aware of the need for improved information sharing and have taken initial steps to facilitate better information sharing within their own territory and across the border, there are some challenges to overcome that would improve information sharing and make the work for CERTs—first-line responders/defenders—more effective, which in turn increases the resilience of critical IT infrastructures globally. But unfortunately, their success often depends on the policy community to organise sharing in a way that is practical and actually helps CERTs in their efforts to prevent and mitigate threats and vulnerabilities. The EU and the US should therefore fund the process towards a joint automatic, standardised open-source threat and vulnerabilities intelligence-sharing solution. The EU and the US should consider including like-minded states such Japan or Australia in this initiative.

Main features: The solution should address the fact that information-sharing currently is too often a one-way street for either the technical community or the policymakers; for example, CERTs alert policymakers to threats. Resilience builds on feedback and learning, so the solution should take this into account. Moreover, the instruments used can be technical, e.g. using a tool/platform. It should be encouraged that certain types of information be shared, and standards be used for the platforms to exchange and share that information (e.g. STIX, TAXII, and Access Control Specification (ACS) v2). Moreover, it should include incentives for different stakeholders to share information efficiently and effectively. The solution should create structures for willing and like-minded stakeholders to respond jointly to threat intelligence. The solution should promote the sharing of information necessary for incident response, e.g. indicator of compromise (hashes, IP addresses, filenames, etc.) as well as mitigation actions or playbooks that support the remediation. The sharing of information should be made as interoperable as possible, e.g. explore using standards such as OASIS STIX. The process is important to identify what information can be shared widely and by which means.

Use cases of some solutions that go into the direction: The US internally created a consensus across the intelligence community and DoD, DHS and Department of Justice national cyber centres as to the types of information to be shared and the standards to be used for the platforms to exchange and share that information (e.g. STIX, TAXII and ACS v2).

Recommendation 3: Practise joint strategic and political assessments of threats and explore responses in a cybersecurity policy simulation

Instruments jointly implemented:

- Cyber dialogue
- Political/strategic threat assessment

[141] Saslow, 'Global Cyber Resilience: Thematic and Sectoral Approaches.'

- Personnel exchanges, e.g. cyber liaison officer
- Specific topical (cooperation) working groups

Joint strategic goals to be addressed:

- Common understanding of threats and vulnerabilities
- Improving response mechanisms and cooperation among a diverse set of stakeholders

In order to improve the understanding of threats and vulnerabilities not only at an operational level through joint bulletins but also on a strategic level, one instrument that is available is political and strategic threat assessments that both EU and US use internally to assess the situation and inform responses. One way to implement this jointly is through the official dialogue using technical bulletins and other information as basis, and then practise on a strategic level whatever threats are similar. Here there is an opportunity to engage with member states before the dialogue to discuss what analysis can be shared. Another approach to practise analysis of threats and responses could be a cybersecurity policy simulation. Here main stakeholders in the EU and US would go through a past scenario or a likely future scenario, explain their political and strategic analysis of the threat and go through their responses. These simulations reveal how the incident is understood by each stakeholder but also offer the opportunity for dialogue on possible ways to react and cooperate in the future. A scenario can even be applied by a political and strategic assessment that was done jointly beforehand. Hence in theory, practising joint threat assessment and responses would mean that the EU and US have identified that X is a joint threat through an analysis done together. Then relevant stakeholders go through a scenario of how their different responses would look and where there is potential to cooperate to achieve a certain political/strategic outcome agreed upon together.

Main features:

- Identify joint threats
- Practise response mechanisms and cooperation

Use cases (only internally):

- 'In the Council Decision of June 24, 2014 for the arrangement for implementation of the solidarity clause, it was decided that in order to regularly assess the threats facing the Union, the European Council may request the Commission, the High Representative for Security Policy, and other Union agencies to produce reports on specific threats which can include cyber threats.'[142]
- 'INTCEN's products include "intelligence assessments", "strategic assessments" and "special reports and briefings". The Hybrid Fusion Cell, created inside the European External Action Service (EEAS) also provides strategic analysis to EU decision makers.'[143]
- US statement for the record—worldwide threat assessment of the US intelligence community presented in Congress and published. It includes a specific section on cyber matters.[144]
- U.K. and U.S. joint review of annual Cyber Management Review in which governmental stakeholders addressed combined activities against common adversaries.[145]

[142] CCDCOE, 'Council Decision of 24 June 2014 on the arrangements for the implementation by the Union of the solidarity clause (2014/415/EU).'
[143] Matthias Monroy, 'EU Intelligence Centre Facing New Challenges,' *Digit Site 36*, 22 March 2019, https://digit.site36.net/tag/hybrid-fusion-cell/.
[144] Daniel R. Coats, 'Statement for the Record – Worldwide Threat Assessment of the US Intelligence Community,' Senate Select Committee on Intelligence, 29 January 2020, https://www.dni.gov/files/ODNI/documents/2019-ATA-SFR---SSCI.pdf.
[145] NSA/CSS, Twitter announcement, 6 August 2020, https://twitter.com/NSAGov/status/1291418899741913090.

Recommendation 4: Joint comparative study on effectiveness of instruments via the TCPRI

Instruments the recommendation draws upon:

- Accountability and evaluation of instruments
- Cybersecurity R&D

Joint strategic goals to be addressed:

- Assisting each other in improving resilience

Both the EU and the US evaluate how effective their instruments are in achieving a policy outcome individually and have applied, as the paper has showed, different instruments to achieve similar goals. 'For example, to achieve greater cybersecurity of critical infrastructure, the US focused on implementing the NIST Framework whereas the EU passed the NIS Directive. These policies have the same end goal, but they try to achieve it with different policy tools. From a public policy analysis perspective, this creates room for case studies that could comparatively study the effect of differing cyber policy approaches to achieve cybersecurity.'[146] The TCPRI was going to be a means to foster exchange on cybersecurity policy; however, it was never implemented. This paper proposed the running of a pilot programme of the TCPRI with the focus on resilience in cyberspace, a joint strategic goal identified in this paper.

Main features:

- Linking policy research to policymaking
- A structure that is transparent and creates legitimacy, collaboration and accountability

Use cases of instruments that are implemented but not in a comparative context:

- The US Cyberspace Solarium Commission report was published march 2020.
- OMB develops and oversees the implementation of policies, principles, standards, and guidelines on information security. This includes: coordinating the development of standards and guidelines under the National Institute of Standards Technology Act and enforcing their adoption in federal agencies;
- The European Commission's Forward Planning of Evaluations and Studies 2017 and beyond e.g. 2017 Assessment of the 2013 Cybersecurity Strategy or 2020 evaluation of NIS Directive

Recommendation 5: Develop targeted exercises and trainings for different stakeholders

- Crisis response plan
- Exercises, competitions and training of responses
- Awareness activities
- Multi-stakeholder consultations

[146] Julia Schuetze, 'How to Operationalise a Transatlantic Cyber Policy Research Initiative (TCPRI),' *EU Cyber Direct*, 30 September 2019, https://eucyberdirect.eu/content_research/1432/.

- Crowd-sourced vulnerability identification via hackathons and bug bounty challenges (with awards)

Joint strategic goals to be addressed:

- Improve response mechanisms and cooperation among a diverse set of stakeholders
- Improve cybersecurity workforce
- Common understanding of threats and vulnerabilities

Simulations have become a means in cybersecurity policy to practise responses, test policy, build relationships, and verify and validate effective and appropriate coordination.[147] In the US government they are a common practice; for example, scenario-based cybersecurity policy simulations have been used to develop incident response Directive 41. In the US, exercise manuals are provided to stakeholders so they can train their responders.[148] In the EU, exercises have also been used to hone technical skills and test responses.[149] Many stakeholders work transatlantically and rely on response mechanisms and cooperation, especially in global cyber incidents. Therefore it is important to have trusted contacts to reach out to. The paper proposes that exercises and trainings should be implemented among different communities between the EU and US strategically, with the joint goal to improve mechanisms of cooperation in incident responses. To determine which joint training is useful, it first needs to be determined which EU and US stakeholders need to work closely together when responding to cyber incidents. Relevant simulations in order to achieve better cooperation and coordination can then be drafted and tested. It should also be taken into account that both the EU and US already use exercises and trainings in the form of hackathons to identify vulnerabilities. A joint implementation of those forms of simulation should be considered, as it may be a means to build relationships with a joint strategic goal of identifying vulnerabilities. Other forms may include simulations with the aim to develop crisis response mechanisms and policies.

Main features:

- Practise or develop response communication channels and roles
- Educate stakeholders on response roles and responsibilities
- Take account of operational and strategic response actors and their interactions

Use cases:

- The US DHS CISA designed the Elections Cyber Tabletop Exercise Package (ECTEP) Situation Manual (SitMan) as part of a strategic effort to increase stakeholder cyber-exercise design capabilities.[150]
- Cyber Training, Readiness, Integration, Delivery and Enterprise Technology (TRIDENT) is a contract vehicle to offer a more streamlined approach for procuring the military's cyber-training capabilities.[151]

[147] DHS, 'National Cyber Incident Response Plan,' December 2016, https://us-cert.cisa.gov/sites/default/files/ncirp/National_Cyber_Incident_Response_Plan.pdf; Alexa King, 'Practice Makes Perfect: Improving Incident Response With Tabletop Exercises,' *FireEye*, 12 August 2019, https://www.fireeye.com/blog/executive-perspective/2019/08/improving-incident-response-with-tabletop-exercises.html

[148] Cybersecurity and Infrastructure Security Agency, 'Elections Cyber Tabletop Exercise Package,' January 2020, https://www.cisa.gov/sites/default/files/publications/Elections-Cyber-Tabletop-Exercise-Package-20200128-508.pdf.

[149] European Commission. 'Cyber Europe 2020 Will Focus on Health,' Shaping Europe's Digital Future, 5 June 2020, https://ec.europa.eu/digital-single-market/en/news/cyber-europe-2020-will-focus-health

[150] Cybersecurity and Infrastructure Security Agency, 'Elections Cyber Tabletop Exercise Package.'

[151] Mark Pomerleau, 'Army Releases $1B Cyber Training Request,' *Fifth Domain*, 12 June 2020, https://www.fifthdomain.com/dod/cybercom/2020/06/12/army-releases-1b-cyber-training-request/?utm_source=Sailthru.

- Incident handling for policymakers—This course is aimed at policymakers and decision-makers. Participants will learn how incident response on a global scale functions and what the preconditions for establishing a successful CSIRT community are.[152]

Recommendation 6: Set up liaison officers at State Department and DHS CISA as well as EEAS and ENISA

Instruments implemented jointly:

- Personnel exchanges, e.g. cyber liaison officer
- Awareness activities

Joint strategic goals to be addressed:

- Improving response mechanisms and cooperation among a diverse set of stakeholders

Cybersecurity policy architectures (who does what)[153] and the policy and strategies are constantly developing and changing in the EU and in the US. In theory, a liaison officer is for example tasked with 'support strategic partnerships by providing top-quality advice, facilitating effective knowledge management, and providing technical assistance to project planning, coordination, monitoring and reporting in any collaboration' and a liaison officer also 'liaises between two organisations to communicate and coordinate their activities by serving as an official go-between for senior officials of both organisations'.[154] The EU internally uses liaison officers for example in migration policy, where they are tasked with 'collecting information to assist third countries in preventing illegal migration flows and to support border management at the EU's external borders'.[155] In cybersecurity policy, liaison officers are already in use as well, particularly in law enforcement. The FBI has done this for example in the fusion centres to engage with private-sector stakeholders in different states.[156] Hence it is an instrument to connect with stakeholders and build awareness about initiatives. It is also an instrument to create closer cooperation and share information, for example the FBI has a liaison officer at Europol to ensure closer cooperation on the operational level.[157] Moreover, member states, for example Germany, have liaison officers in the Ministry of the Interior in the Department of Homeland Security working on cyber issues. Hence this is an instrument used for closer strategic and operational cooperation. However, outside of cybercrime cooperation between the EU and US, liaison officers are not implemented yet. For example, a liaison officer between the EEAS and the State Department could be beneficial for the awareness of any strategic development of cyber policy and joint responses. A liaison officer of ENISA at DHS CISA and vice versa would be beneficial for creating joint situational awareness on the threat and vulnerability landscape and fostering multi-stakeholder work on cybersecurity best practices. In both areas, sharing confidential information is as

[152] FIRST, 'Trainings – Incident Handling for Policy Makers,' https://www.first.org/education/trainings.

[153] Sven Herpig and Rebecca Beigel, 'Staatliche Cybersicherheitsarchitektur,' *Stiftung Neue Verantwortung*, March 2020, https://www.stiftung-nv.de/sites/default/files/snv_graph_2runde_20200603.pdf; Charlie Mitchell, 'National Cyber Director Debate Raises Broader Issue: Is a Major Overhaul Needed at DHS?,' *Inside Cybersecurity*, 24 July 2020, https://insidecybersecurity.com/share/11468.

[154] Cloud Security Alliance, 'Roles and Responsibilities for Liaison Officer,' April 2012, https://downloads.cloudsecurityalliance.org/standards/ISC_Liaison_Office_Role_Responsibilities.pdf.

[155] Council of the European Union, 'Immigration Liaison Officers: Council Adopts New Rules to Improve Coordination,' 14 June 2019, https://www.consilium.europa.eu/en/press/press-releases/2019/06/14/immigration-liaison-officers-council-adopts-new-rules-to-improve-coordination/.

[156] Federal Bureau of Investigation, 'Office of Partner Engagement,' https://www.fbi.gov/about/partnerships/office-of-partner-engagement.

[157] Europol. 'FBI Director James Comey: 'Standing Together, We Are Unbreakable,' 24 September 2015, https://www.europol.europa.eu/newsroom/news/fbi-director-james-comey-%E2%80%9Cstanding-together-we-are-unbreakable%E2%80%99%E2%80%99. Since May 2015, the FBI has deployed a permanent liaison officer to Europol's headquarters in The Hague, strengthening the cooperation between the two agencies and further ensuring the fast and effective exchange of information.

important as law enforcement. Liaison officers should ensure better understanding of what each side is dealing with. The purpose should be on exchange of best practices, networking and coordinating, e.g. getting the right people together to work on joint goals. As this paper has shown, there are important strategic joint goals on resilience and on strategic response that need the development and building of sustainable and trustful relationships, bringing together the stakeholders working on different policy and strategic issues.

Main features:

- Build multi-stakeholder relationships
- Share information to achieve joint strategic goals
- Create awareness about policy initiatives and foster knowledge management

Use cases:

- FBI liaison in fusion centres
- FBI liaison at Europol working on cybercrime

Recommendation 7: Work together on global guidelines/frameworks for cybersecurity skills development

Instruments implemented jointly:

- Capacity building in third countries
- Specific topical (cooperation) working groups
- Cybersecurity R&D
- Provision of guidelines/frameworks for standardisation and taxonomy
- Gathering and sharing of best practices

Joint strategic goals to be addressed:

- Improve cybersecurity workforce

The EU and the US have realised that a larger cybersecurity workforce is needed to meet the demands from private sector and government and to fulfil policy objectives such as the protection of the economy or national security.[158] Both the EU and the US have thus far approached the issue separately but started with the same approach, to first look at what skills are required and then to think on how to develop it. While the US has already established a skillset framework, the NICE framework,[159] and has set up several initiatives such as the federal registry for cybersecurity, an assessment of which positions are currently available and which can be retrained,[160] the EU is starting its own Working Group on the European

[158] 'The cybersecurity workforce shortage and skills gap is a major concern for both economic development and national security, especially in the rapid digitization of the global economy.' European Union Agency for Cybersecurity, 'European Cybersecurity Skills Framework,' ENISA, 2020, https://www.enisa.europa.eu/topics/cybersecurity-education/european-cybersecurity-skills-framework. 'The federal government needs a qualified, well-trained cybersecurity workforce to protect vital IT systems. Not having enough of these workers is one reason why securing federal systems is on our High Risk list.' US Government Accountability Office, 'Cybersecurity Workforce: Agencies Need to Accurately Categorize Positions to Effectively Identify Critical Staffing Needs,' 12 March 2019, https://www.gao.gov/products/GAO-19-144.

[159] National Initiative for Cybersecurity Careers and Studies, 'NICE Cybersecurity Workforce Framework,' https://niccs.us-cert.gov/about-niccs/featured-stories/nice-cybersecurity-workforce-framework.

[160] Executive Office of the President, 'America's Cybersecurity Workforce,' *Federal Register*, 9 May 2019, https://www.federalregister.gov/documents/2019/05/09/2019-09750/americas-cybersecurity-workforce.

Cybersecurity Skills Framework.[161] There is a strong interest in learning from each other and working together on the topic of skills framework to give a more unified standard for the knowledge and skills necessary for persons that aim to build a career in cybersecurity and for companies that need to frequently hire cybersecurity staff across countries. Therefore, the recommendation is to include US stakeholders in the process of developing an EU skills development framework but with the aim to identify which of those skills have the potential to become global standards and which may be unique to the EU or US. This work also has potential to be connected to EU and US cybersecurity capacity work, as the EU and US could work together with developing countries in identifying which skills are essential for the unique threats and vulnerabilities they face. Instruments to achieve this are, for example, best practice sharing or a working group on the topic.

Main features:

- Harmonising taxonomies
- Building a global cybersecurity workforce with translatable skills

Use cases:

- The European Skills, Competences, Qualifications and Occupations (ESCO) skills hierarchy is partially based on elements of the existing classification of O*Net of the US Department of Labor, and the Canadian skill and knowledge glossary.[162]
- The European Qualifications Framework (EQF) was identified as 'a translation device – a converter or reading grid – making it possible to position and compare learning outcomes'[163]. In the project TRACE (Transparent Competences in Europe), scientists were working with Skillsnet on the O*Net framework developed in the US and have carried out a feasibility analysis on its potential contribution to the TRACE translator tool.[164]

[161] European Union Agency for Cybersecurity, 'European Cybersecurity Skills Framework.'
[162] European Commission, 'Skills/Competences,' ESCO, 2020, https://ec.europa.eu/esco/portal/skill.
[163] TRACE, 'Overview of European Competency Frameworks,' 2012, http://www.menon.org/wp-content/uploads/2012/11/9.-TRACE-Overview-of-EU-competency-frameworks1.pdf.
[164] TRACE, 'Overview of European Competency Frameworks.'

How can EU and US achieve their joint strategic goals?

7 recommendations

01

Develop joint technical bulletins

02

Fund a process to develop joint automatic, standardised open-source threat and vulnerabilities intelligence-sharing solutions

03

Practise joint strategic and political assessments of threats and explore responses in a cybersecurity policy exercise

04

Joint comparative study on effectiveness of policy instruments in achieving strategic outcomes

05

Develop targeted exercises and trainings for differents stakeholders

06

Set up liaison officers in crucial institutions

07

Work together on global guidelines/frameworks for cybersecurity skills development

9. Next steps for policymakers

The paper proposes that the joint actions be developed further in detail in a multi-stakeholder process, and discussed by policymakers and diplomats at the next EU–US Cyber Dialogue. Policymakers should do two things:

- Rank which recommendations should be implemented first
- Formulate implementation details in a multi-stakeholder format

Furthermore, the instruments that are unique to the EU or the US and the instruments where there are limitations for joint implementation and ongoing exchange should be taken into account to achieve a better understanding of the divergences of cybersecurity policy and the reasons for it. The instruments that now have higher limitations for joint implementation may become available for joint actions in the future when limitations are addressed internally, or can be used in other ways, for example in a coordinated effort by the EU and member states together. An overview of which those are can be found in the annex. In order to achieve this, the paper recommends work on clarification of goals that could be shared but whose definitions may not have the same meaning. A specific strategic goal is deterrence, with the wording 'influence behavior' and 'peace and security' in the US context and 'stability of cyberspace' in the EU context. When those strategic goals are defined, further work on potential joint goals will be possible.

Abbreviations

5G	fifth-generation technology standard for cellular networks
ACS	Access Control Specification
CERT	Computer Emergency Response Team
CFSP	Common Foreign and Security Policy
CISA	Cybersecurity and Infrastructure Security Agency
CSIRT	Computer Security Incident Response Team
CTI	cyber-threat indicator
CUI	controlled unclassified information
CVD	coordinated vulnerability disclosure
DHS	Department of Homeland Security
DM	defensive measure
DoD	(US) Department of Defense
DoE	(US) Department of Energy
DSP	digital service provider
ESSA	Enhance Shared Situational Awareness
EC3	European Cybercrime Centre
EEAS	European External Action Service
ENISA	European Union Agency for Cybersecurity
EO	Executive Order
EU INTCEN	EU Intelligence and Situation Centre
FBI	Federal Bureau of Investigation
FISMA	Federal Information Security Management Act
FY	financial year
HR/VP	High Representative of the Union for Foreign Affairs and Security Policy
IoT	Internet of Things
IT	information technology
MISP	Malware Information Sharing Platform
NCCIC	National Cybersecurity and Communications Integration Center
NICE	National Initiative for Cybersecurity Education
NIS	network and information systems
NIST	National Institute of Standards and Technology

NSA	National Security Agency
NTIA	National Telecommunications and Information Administration
OFAC	Office of Foreign Assets Control
PII	personally identifiable information
PESCO	Permanent Structured Cooperation
R&D	research and development
TCPRI	Transatlantic Cyber Policy Research Initiative
UNGGE	UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security

About the author

Julia Schuetze works on cyber diplomacy of the European Union with the United States and Japan as part of the EU Cyber Direct project. She alsoworks as project manager of the "Transatlantic Cyber Forum" which deals with internationalcyber security policy. Her research focus is on cyber operations against electoral processes, comparative cybersecurity policy and governance. As part of her role at SNV she has spoken at the Congressional Cybersecurity Caucus in the United States, has facilitated workshops on Germany's cybersecurity architecture with the foreign office, has organized the cybersecurity conference with the Bundesakademie für Sicherheitspolitik as well as several other workshops and events with U.S. and German cybersecurity experts in Washington D.C. and Berlin. Her work has been published or cited by news outlets, such as WirtschaftsWoche Der Tagesspiegel, F.A.Z and the BBC. She is a Cybersecurity Policy Fellow at New America Foundation and volunteers for the OGP Civil Society Working Group and for the Steering Committee of the Internet Governance Forum Germany.

About EU CyberDirect

The **EU Cyber Direct** project supports EU cyber diplomacy efforts and consequently contributes to the development of a secure, stable and rules-based international order in cyberspace through extensive dialogues with strategic partner countries and regional/international organisations. The **EU Cyber Direct** is funded by the European Commission under the Partnership Instrument, International Digital Cooperation project: Trust and Security in Cyberspace.

RESEARCH IN FOCUS

is a series of research papers aimed at supporting the EU's cyber-related policies by providing a timely and policy-relevant analysis.

EU CYBER DIRECT

This project is funded by the European Union.