Bendiek, Annegret; Schulze, Matthias

Research Report

Attribution: A major challenge for EU cyber sanctions. An analysis of WannaCry, NotPetya, Cloud Hopper, Bundestag Hack and the attack on the OPCW

SWP Research Paper, No. 11/2021

Provided in Cooperation with:
Stiftung Wissenschaft und Politik (SWP), German Institute for International and Security Affairs, Berlin

Suggested Citation: Bendiek, Annegret; Schulze, Matthias (2021) : Attribution: A major challenge for EU cyber sanctions. An analysis of WannaCry, NotPetya, Cloud Hopper, Bundestag Hack and the attack on the OPCW, SWP Research Paper, No. 11/2021, Stiftung Wissenschaft und Politik (SWP), Berlin,
https://doi.org/10.18449/2021RP11

This Version is available at:
https://hdl.handle.net/10419/253242

SWP

SWP Research Paper

Annegret Bendiek and Matthias Schulze

Attribution: A Major Challenge for EU Cyber Sanctions

An Analysis of WannaCry, NotPetya, Cloud Hopper, Bundestag Hack and the Attack on the OPCW

Stiftung Wissenschaft und Politik
German Institute for International and Security Affairs

SWP Research Paper 11
December 2021, Berlin

- The attribution of cyberattacks is a sovereign act by the EU Member States. However, these all have different technical and intelligence capabilities. This leads to a lack of coherence in European cyber diplomacy, for example when imposing cyber sanctions.
- Analysis of policy responses to the WannaCry, NotPetya, Cloud Hopper, OPCW, and Bundestag hack cyber incidents reveals the following problems: Attribution takes a long time and relies on intelligence from NATO partners; the technical realities and the legal facts for classifying and prosecuting cyberattacks do not always match; the weighting of the criteria for establishing what constitutes a crime is unclear.
- Cyber sanctions should be proportionate, targeted measures and destructive attacks, such as WannaCry or NotPetya, should result in harsher punishment than everyday cases of cyber espionage, such as Cloud Hopper or the Bundestag hack. The EU must adapt its tools accordingly.
- The EU should tighten the legal criteria and harmonise the standards of evidence for attribution. The EU Joint Cyber Unit and EU INTCEN, part of the European External Action Service, should be strengthened to improve the exchange of forensic information and to coordinate attribution policy more effectively.
- EU Member States and their allied partners should better coordinate political signalling to condemn cyberattacks. To this end, it would make sense to allow qualified majority voting for the adoption of cyber sanctions.

SWP Research Paper

Annegret Bendiek and Matthias Schulze

Attribution: A Major Challenge for EU Cyber Sanctions

An Analysis of WannaCry, NotPetya, Cloud Hopper, Bundestag Hack and the Attack on the OPCW

Stiftung Wissenschaft und Politik
German Institute for International and Security Affairs

SWP Research Paper 11
December 2021, Berlin

SWP Research Papers are
peer reviewed by senior
researchers and the execu-
tive board of the Institute.
They are also subject to fact-
checking and copy-editing.
For further information
on our quality control pro-
cedures, please visit the
SWP website: https://
www.swp-berlin.org/en/
about-swp/quality-
management-for-swp-
publications/.
SWP Research Papers reflect
the views of the author(s).

SWP
Stiftung Wissenschaft und
Politik
German Institute
for International
and Security Affairs

Ludwigkirchplatz 3—4
10719 Berlin
Germany
Phone +49 30 880 07-0
Fax +49 30 880 07-200
www.swp-berlin.org
swp@swp-berlin.org

ISSN (Print) 2747-5123
ISSN (Online) 1863-1053
doi: 10.18449/2021RP11

(English version of
SWP-Studie 17/2021)

Table of Contents

5 Issues and Recommendations

7 EU Cyber Diplomacy and the Problem of Attribution

10 The Politics of Attribution
14 What is a serious cyberattack against the EU?
14 Which institutions and procedures determine attribution?
16 The cyber diplomacy toolbox: A step-by-step plan

20 Case Studies: EU Cyber Sanctions and Their Attribution
20 WannaCry 2017
23 NotPetya 2017
26 Operation Cloud Hopper 2016
29 Bundestag Hack 2015
32 Attempted attack on the OPCW 2018

34 Shortcomings of the Attribution Policy

37 Conclusions

39 Appendix
39 Glossary
42 Abbreviations
42 Comparison table of cases (online only)

Dr Annegret Bendiek is Deputy Head of EU / Europe Research Division.
Dr Matthias Schulze is Deputy Head of the International Security Research Division.

Attribution: A Major Challenge for EU Cyber Sanctions. An Analysis of WannaCry, NotPetya, Cloud Hopper, Bundestag Hack and the Attack on the OPCW

The European Union first imposed what were referred to as "cyber sanctions" against individuals associated with the Russian, North Korean and Chinese government in July 2020. The measures include travel bans and asset freezes. They apply across the EU 27 and have been adopted as a diplomatic or political response to malicious cyber operations against the EU. Cyber sanctions are only *one* of the common diplomatic instruments that are part of the EU's cyber diplomacy toolbox. Their intensity is adjusted to stay below the threshold for armed conflict. Since 2017, EU Member States have been using this toolbox to try to respond to serious cyber operations in a coordinated way under the Common Foreign and Security Policy (CFSP). However, demonstrating and implementing a proportionate, coherent and, above all, legally justified EU response to cyberattacks is highly challenging. The diplomatic response must be consistent from a legal, technical and political perspective, in the event that listed individuals challenge the EU's restrictive measures (financial sanctions or travel restrictions) in court. Under Article 263 IV of the Treaty on the Functioning of the European Union (TFEU), the targets of such punitive measures enjoy full legal protection from the European Court of Justice (ECJ).

If the EU wants to impose legitimate cyber sanctions, it first needs to determine the origin (attribution) of cyberattacks in a careful and reasonable manner. However, at EU level, the process of attribution, i.e. the technical, legal and political assignment of individual responsibility for cyberattacks, is incoherent and partly contradictory. The reasons for this are manifold. Attribution is a sovereign act of the Member States which have varying technical and intelligence capabilities. The EU's role is only to coordinate, collect forensic evidence and share intelligence among the Member States and EU institutions. Given the increasing number and intensity of attacks in the cyber and information domain space (CIR), attribution is key. It is also necessary to be able to uphold the principle of responsible state behaviour which the EU promotes.

The central question this study seeks to answer is therefore: How does the process of attribution of cyberattacks, from a legal, technical and political perspective, function in the EU? What are the shortcomings, inconsistencies and contradictions in this process? What are the implications for the EU's adoption of cyber sanctions? What lessons learned can be derived from the analysis of historical cases where sanctions were implemented? The study analyses five specific cyberattacks against the EU (WannaCry 2017, NotPetya 2017, Operation Cloud Hopper 2016, the 2015 Bundestag hack, and the 2018 attack on the Organization for the Prohibition of Chemical Weapons, which was prevented) and finds:

First, the EU's attribution capacity is highly dependent on intelligence sharing with the US and the UK. While the Five Eyes intelligence alliance (consisting of the US, the UK, Canada, Australia and New Zealand) coordinates its attribution and public naming and shaming in a manner which has a high media impact, the coordination processes in the EU 27 are naturally slower: months, if not years, pass between a cyber incident and the implementation of sanctions. To increase the effectiveness of political signalling, attribution must occur more quickly and coordination among Member States must be stepped-up.

Second, the legal framework developed for EU cyber sanctions does not always reflect the technical realities of cyber operations. The criteria that a cyber incident must fulfil in order to justify legal sanctions need to be honed. A greater distinction should be made between successful attacks and attempts. The criminal intent and the strategic motivation of attacks can rarely be inferred from technical indicators alone. Nevertheless, technical indicators are key for the legal assessment of an attack and the subsequent justification of a sanction decision. Therefore, technical and legal language should be harmonised.

Thirdly, cyber incidents should be more clearly differentiated according to their intensity and technical characteristics in order to tailor the EU's diplomatic response to ensure it is proportional: WannaCry and NotPetya caused billions of dollars of damage worldwide and could have resulted in much harsher punitive measures than asset freezes.

Fourthly, EU Member States would be well advised to harmonise the criteria required for attribution. Furthermore, attribution evidence should be more transparent, without jeopardising intelligence access. All Member States should use a comparable standardised system (probability yardstick) to enable a classification of responsibility.

Finally, information on indicators of compromise (IoCs), i.e. characteristics and data indicating that a system or network has been compromised, must be made available to all stakeholders through the Joint Cyber Unit in the EU Commission and the EU INTCEN within the European External Action Service (EEAS). Both institutions should be strengthened in terms of competence in order to improve cyber intelligence.

Against this background, the German government would be advised to actively support the French Presidency's initiative to reform the EU Cyber Diplomacy Toolbox so that attacks on the EU's critical infrastructure, supply chains and democratic institutions can be more effectively countered in future. This is in line with the requirements for the implementation of the December 2020 Cybersecurity Strategy.

EU Cyber Diplomacy and the Problem of Attribution

Since 2013, the European Union has been developing policy and regulatory measures to respond to "malicious" cyber operations directed against the EU from third countries (cybersecurity by law).[1] Within the framework of its cyber diplomacy, the EU advocates the peaceful resolution of international disputes and emphasises the importance of a "global, open, free, stable and secure cyberspace".[2] This stance already shaped the first cybersecurity strategy in 2013 and was most recently confirmed in December 2020 with the current strategy.[3] The stated aim is to maintain the stability, security and benefits of the Internet and to guarantee the use of information and communication technologies.[4] Since then, the EU Member States have played a key role in multilateral forums, such as the Governmental Group of Experts and the Open Ended Working Group at United Nations (UN) level, in anchoring cyber norms in current international law and establishing and enforcing a rules-based international order in the cyber and information space (CIR).[5] In 2015, the international community agreed that a response to cyberattacks should be proportional, i.e. that counterreactions are only legitimised under international law if the attacks are of a certain scale and produce certain effects, i.e. are similar in intensity to an armed attack. The requirement of proportionality includes, for example, refraining from cyber operations against critical infrastructures. Active cyber defence is permitted if states fail to fulfil their due diligence obligations. These norms guide the EU's actions.[6]

1 We owe the key findings of this study to the in-depth research of Anna Sophia Tiedeke, Kerstin Zettl and Andreas Schmidt. The aforementioned contributed significantly to the development of this SWP study through their analyses in the context of the pilot project on the feasibility of a repository on cyber incidents in Europe in cooperation with the Cyber Foreign Policy Staff in 2020/21. Special thanks also go to Veronika Datzer for her revisions.
The attacks are "WannaCry", "NotPetya", "Operation Cloud Hopper", "Bundestag hack" and "attempted attack on the Organization for the Prohibition of Chemical Weapons (OPCW)". The EU classified these attacks as malicious cyberattacks and attempted cyberattacks with a potentially significant impact "posing an external threat to the Union or its Member States".

2 Council of the European Union, *Council Conclusions on Malicious Cyber Activities – Endorsement Approval*, Brussels, 16 April 2018, https://data.consilium.europa.eu/doc/document/ST-7925-2018-INIT/en/pdf.

3 Annegret Bendiek and Matthias C. Kettemann, *Revisiting the EU Cybersecurity Strategy: A Call for EU Cyber Diplomacy*, SWP Comment 16/2021 (Berlin: Stiftung Wissenschaft und Politik, February 2021), https://www.swp-berlin.org/publications/products/comments/2021C16_EUCyberDiplomacy.pdf; Annegret Bendiek, Raphael Bossong and Matthias Schulze, *The EU's Revised Cybersecurity Strategy. Half-Hearted Progress on Far-Reaching Challenges*, SWP Comment 47/2017, (Berlin: Stiftung Wissenschaft und Politik, November 2017), https://www.swp-berlin.org/publikation/revised-cybersecurity-strategy; Annegret Bendiek, *Tests of Partnership. Transatlantic Cooperation in Cyber Security, Internet Governance, and Data Protection*, SWP Research Paper 5/2014 (Berlin: Stiftung Wissenschaft und Politik, March 2014), https://www.swp-berlin.org/publikation/transatlantic-cooperation-in-cyber-security.

4 Council of the European Union, *Council Conclusions on Malicious Cyber Activities* (see note 2), 2.

5 See Matthias Schulze, *Konflikte im Cyberspace* Berlin: United Nations Association of Germany, 2020 (UN-Basis-Information 61), https://dgvn.de/veroeffentlichungen/publikation/einzel/konflikte-im-cyberspace/ (accessed 6 May 2021); Alex Grigsby, "The End of Cyber Norms", *Survival* 59, no. 6 (2017): 109–22.

6 See Annegret Bendiek, *Due Diligence in Cyberspace. Guidelines for International and European Cyber Policy and Cybersecurity Policy*, SWP Research Paper 7/2016 (Berlin: Stiftung Wissenschaft und Politik, May 2016), https://www.swp-berlin.org/publikation/due-diligence-in-cyberspace; *European Digital Sovereignty: Combining Self-interest with Due Diligence,* EU Policy Brief 5 (Ottawa: Centre for European Studies, Carleton University, December 2020), https://carleton.ca/ces/wp-content/

Since the spectacular cyber operations WannaCry and NotPetya (both in spring 2017), the political pressure to take action has increased.[7] WannaCry is considered to be one of the most extensive cyberattacks to date with "victims" in over 150 countries. NotPetya is one of the most costly and destructive attacks to date.[8] In June 2017, the Council of the EU agreed in a CFSP decision to develop a "diplomatic response framework" (known as the cyber diplomacy toolbox) to enable the Union to demonstrate a common, coordinated diplomatic counterresponse to serious cyber incidents below the threshold of armed conflict. Attackers are to be persuaded to refrain from attacks against the EU through threats of retaliation ("naming and shaming"). The Council consequently announced in April 2018 that it would no longer tolerate the misuse of information and communication technology (ICT) for "malicious" purposes.[9] On 17 May 2019, the cyber sanctions regime was completed with Regulation (EU) 2019/796 on restrictive measures against cyber-attacks.[10]

In July 2020, years after the initial incidents, the Council of the EU imposed cyber sanctions against the North Korean, Chinese and Russian citizens deemed responsible for WannaCry, Cloud Hopper and NotPetya, respectively.[11] The delay is explained in part by the fact that determining the responsibility of cyberattacks is technically and legally challenging because it requires IT forensic and intelligence capabilities. Only a few Member States, including Sweden, the Netherlands, Estonia, Austria, France and Germany, have these attribution capabilities and the political will to share information with other Member States via EU INTCEN, the intelligence analysis unit of the European External Action Service (EEAS). A prerequisite for Brussels to issue sanctions in response cyberattacks is that the EU can plausibly prove the originator and the "malicious" intent. This is a rather complex undertaking, not only because of the decentralised structure of the cyber and information space, but also because of the different starting conditions in the Member States and the lack of analytical capabilities in the EEAS or at EU level.

A collective, common process of attribution takes place only sporadically within the EU.

Attribution is a central problem in cyber conflict research and poses a particular challenge for EU cyber diplomacy and its cyber sanctions regime.[12] Security policy and the attribution of cyberattacks are the prerogative of EU Member States. These are reluctant to share sensitive intelligence at the EU level, as this allows inferences about national cyber defence capabilities. Sharing intelligence could compromise state sources and access to classified information. A collective, shared process of attribution occurs only sporadically within the EU: As a rule, each Member State attributes autonomously. The EU merely tries to pool the relevant information and coordinate the political response to cyberattacks. This circumstance makes it difficult for the Member States to act together to name and shame attackers in EU cyber diplomacy. Notwithstanding, coordinated attribution between Member States and EU institutions is a necessary precondition for activating the EU diplomatic response framework and sanctions.

A fragmented attribution process weakens the credibility, legitimacy and effectiveness of EU cyber diplomacy. A lack of coherence when it comes to measures is one consequence: the Russian intelligence officers who were subject to cyber sanctions in the form of travel bans and asset freezes in 2020 had already been subject to the same restrictive measures under a different EU sanctions regime a few years

uploads/Bendiek-EU-Policy-Brief-Digital-Sovereignty-2.pdf (accessed 4 June 2021).

7 Other EU security policy initiatives include the Cyber Defence Policy Framework (2018), the EU Cybersecurity Act and the 5G Toolbox (both 2019), the Security Union Strategy and the FDI Screening Regulation (2020).

8 Andy Greenberg, "White House Blames Russia for NotPetya, the 'Most Costly Cyberattack in History'", *Wired* (online), 15 February 2018, https://www.wired.com/story/white-house-russia-notpetya-attribution/ (accessed 18 May 2021).

9 Council of the European Union, *Council Conclusions on Malicious Cyber Activities* (see note 2).

10 Ibid.

11 Council of the European Union, *Council Decision (CFSP) 2020/1127 of 30 July 2020 Amending Decision (CFSP) 2019/797 Concerning restrictive Measures against Cyber-attacks Threatening the Union or Its Member States* https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32020D1127&from=DE (accessed 2 June 2021). On the legal basis of Article 13(1) of Regulation (EU) 2019/796, Annex I to Regulation (EU) 2019/796 amended the list of natural and legal persons, entities and bodies referred to in Article 3 of Regulation (EU) 2019/796.

12 See Florian J. Egloff and Max Smeets, "Publicly Attributing Cyber Attacks: A Framework", *Journal of Strategic Studies,* (2021): 1—32.

earlier. The measures were therefore duplicative and had no additional effect.[13] Moreover, apart from the redundancy of this step, it is questionable to what extent travel restrictions and frozen accounts really have a deterrent effect on aggressors or are ultimately just symbolic politics.[14] Moreover, the effectiveness and legitimacy of cyber sanctions suffer if the public naming and shaming of the perpetrators of cyberattacks is not supported by Member State governments.

It is up to each government to decide whether to follow the attributions published by other EU countries.

It is up to each government to decide whether it will endorse the attributions published by other EU states, whether through diplomacy or the media. For example, only six of the 27 EU states have reaffirmed the 2020 sanctions against Russia through government or diplomatic statements.[15] Although Germany helped to initiate cyber sanctions at the EU level after the 2015 Bundestag hack, the German government has been slow to publicly condemn the perpetrators. This half-heartedness unnecessarily diminishes the signalling effect of cyber sanctions. Given the unanimity requirement in the Council, a lack of coherence in signalling reduces the impact of punitive measures. As a result, cyberattackers are currently not sufficiently deterred from perpetrating attacks.[16] The veto right and the polyphony of the Member States also damage the foreign policy credibility of the Europeans in international cyber diplomacy as well. As a result, EU states are undermining the principle of "due diligence" that was agreed upon within the framework of the United Nations.

The EU and the French government have announced that they will evaluate the cyber diplomacy toolbox, including the cyber sanctions, in the upcoming Council Presidency. When the EU imposes sanctions, it must comply with minimum standards of the rule of law vis-à-vis the individuals concerned. This is accompanied by qualitative requirements for attribution. In the following sections, this study will outline the urgency of reforming the diplomatic response framework and identify starting points for its redesign. To this end, it will first examine the cyber incidents that first triggered the cyber sanctions regime at the EU level in 2020, namely the 2015 Bundestag hack, WannaCry, NotPetya (both 2017), the attack on the Organisation for the Prohibition of Chemical Weapons (OPCW), and Operation Cloud Hopper. The focus is on how coherently the EU has classified these attacks from a technical, legal and political perspective. What the paper does not analyse, however, is the operational procedures of attribution between the security agencies, the exchange of information and knowledge between them, and the effectiveness of the sanctions regime in terms of its impact on the targets.

13 Stefan Soesanto, "Europe Has No Strategy on Cyber Sanctions", *Lawfare*, 20 November 2020, http://www.lawfareblog.com/europe-has-no-strategy-cyber-sanctions (accessed 6 May 2020).

14 Annegret Bendiek, Minna Ålander and Paul Bochtler, *CFSP: The Capability-Expectation Gap Revisited. A Data-based Analysis*, SWP Comment 58/2020 (Berlin: Stiftung Wissenschaft und Politik, November 2020), https://www.swp-berlin.org/publikation/cfsp-the-capability-expectation-gap-revisited; see also Francesco Giumelli, Fabian Hoffmann and Anna Książczaková, "The When, What, Where and Why of European Union Sanctions", *European Security* 30, no. 1 (2021): 1—23; Niklas Helwig, Juha Jokela and Clara Portela, eds., *Sharpening EU Sanctions Policy for a Geopolitical Era* (Helsinki: Prime Minister's Office, 2020), https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/162257/VNTEAS_2020_31.pdf (accessed 4 June 2021); Clara Portela et al., "Consensus against All Odds: Explaining the Persistence of Sanctions on Russia", *Journal of European Integration* 43, no. 6 (2020): 1—17.

15 Soesanto, "*Europe Has No Strategy on Cyber Sanctions*" (see note 13).

16 Erica D. Borghard and Shawn W. Lonergan, "The Logic of Coercion in Cyberspace", *Security Studies* 26, no. 3 (2017): 452—81 (463).

The Politics of Attribution

Attribution describes the process of assigning responsibility for a cyberattack to an actor. The key question is: who did it?[17] The reliability of attribution changes over time as knowledge about a cyber incident gradually increases and uncertainty about responsibility potentially decreases. The more time and analytical skills available, the greater the certainty of attribution tends to be. The process has three levels: technical, legal and political (see Figure 1, p. 11). These build on each other, but sometimes their goals are conflicting:

The combination of these three levels can be defined as the *policy of attribution*. This refers to the process of technical and legal classification and public (non-) naming of the perpetrators of a cyberattack as well as the initiation of countermeasures.

After a cyber incident, the first step is *technical attribution*. This involves using IT forensics to evaluate technical artefacts and evidence such as network logs or malware traces (known as indicators of compromise, IoCs) in the computers affected by the attack. These are compared with the tools, techniques/tactics and procedures (TTP) of past incidents and then correlated with each other. Based on this, competing hypotheses about attackers can be generated, similar to what happens in criminal investigations. Put simply, the goal of technical attribution is to gather knowledge about the attacker's actions ("knowing the attacker"). This process is tactical in nature, as it is difficult to infer the strategic or political motivation for a cyber incident from simple network artefacts.[18] It is also difficult to conclusively answer the "socio-political question" of who was sitting at the computer and on whose behalf an attacker acted. Malware recycling among different hacker groups is a common phenomenon. Therefore, technical analysis alone cannot provide a direct answer as to who was behind an attack. Technical indications such as system language settings can provide clues, but they can also be deliberate false flags.[19]

In the course of the processes of legal and political attribution, which are not always clearly distinguishable, the attacked state tries to answer more actor-related questions: Which person or organisation is responsible for the hack? Who gave the order for it? What was the strategic or political motivation behind the operation? Here, the focus is no longer on purely technical indicators, but also on political factors such as national security strategies and geopolitical contexts.[20] The core element of *political attribution* is the "naming and shaming" of the attacker, either bilaterally through non-public diplomatic channels or publicly, with the aim of exposing an aggressor. The goal of this political attribution is that the perpetrator will reconsider his or her behaviour and refrain from future attacks. Political attribution can thus also be *public attribution*, for example in conjunction with allies and partners, with a view to strengthening the legitimacy of condemning a perpetrator before the international public. However, a state may also deliberately refrain from public attribution if this does not seem opportune under the prevailing political circumstances, for example during a political crisis, if the evidence is thin or if its own sources are in danger of becoming compromised.[21] Moreover, a state which engages in public attribution may have to reckon with countermeasures, such as sanctions. Political attribution thus always takes place in the context of international relations and power dynamics. Political attribution often requires a "judgement call", because the

17 Thomas Rid and Ben Buchanan, "Attributing Cyber Attacks", *Journal of Strategic Studies* 38, no. 1–2 (2014): 4–37 (4).

18 Ryan Stillions, "The Detection Maturity Level Model", *Ryan Stillions Blogspot*, 22 April 2014, http://ryanstillions.blogspot.com/2014/04/the-dml-model_21.html (accessed 1 January 2020).

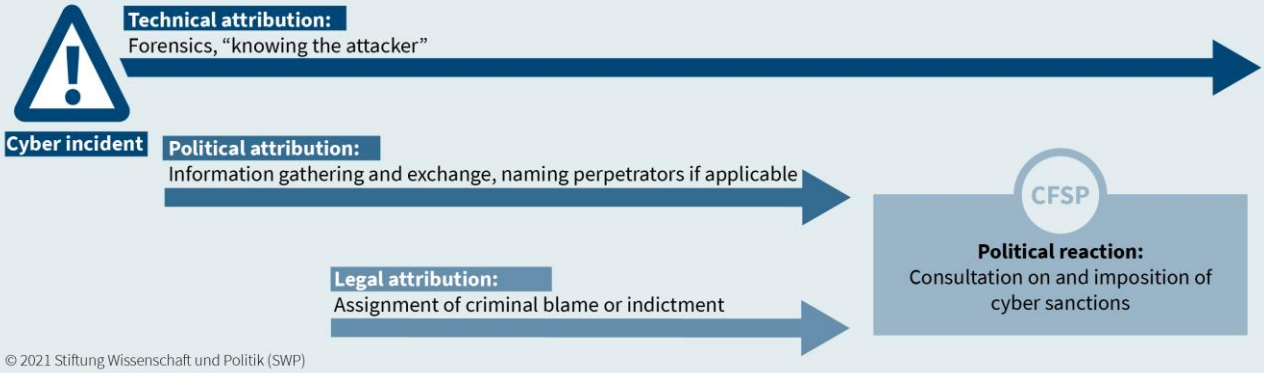
19 Erik Gartzke and Jon R. Lindsay, "Weaving Tangled Webs. Offense, Defense, and Deception in Cyberspace", *Security Studies* 24, no. 2 (2015): 316–48.

20 Jason Healey, *Beyond Attribution: Seeking National Responsibility in Cyberspace*, Issue Brief (Washington, D.C.: Atlantic Council, 22 December 2012), https://www.atlanticcouncil.org/publications/issue-briefs/beyond-attribution-seeking-national-responsibility-in-cyberspace (accessed 15 September 2021).

21 Egloff and Smeets, "Publicly Attributing Cyber Attacks" (see note 12).

Figure 1

Three levels of attribution
The determination of authorship and responsibility



technical indicators are not clear. Political attribution thus aims not only at knowing who the aggressor is, but also at naming them.

Legal attribution is essential and indispensable if the goal is a legitimate policy response to cyber incidents. Legal attribution describes the assignment of criminal blame or indictment. Political attribution and legal attribution of responsibility are formally distinct actions under international law.[22] The distinction between individual and state responsibility is important.[23] A necessary precondition of any legal attribution of responsibility is the legal classification of the incident: cybercrime is to be treated according to different legal statutes than a crime under international law. Cybercrime allows for individual sanctions, whereas an act in violation of international law can also legitimise collectively effective restrictive measures under precisely defined circumstances. Cybercrime is, in turn, also to be distinguished from cyberespionage, which is not prohibited under international law but can be punished individually under criminal law. And this, in turn, is to be distinguished from cyberattacks crossing the threshold of an armed attack, which are illegal under international law according to Article 2.4 of the UN Charter. The latter can even trigger the right of self-defence under Article 51 of the UN Charter and justify the use of military responses.

An adequate and proportionate legal response to cyberattacks requires detailed technical and policy competencies to classify incidents. States may legally assess the same cyber incident differently depending on their detection and investigation capabilities — for example by classifying the same incident either as cybercrime or as a covert espionage operation. Moreover, depending on the classification, there are also different requirements for evidentiary standards. Legal attribution also aims to hold individuals, the people behind the machine, accountable through the mechanisms of law enforcement. Higher standards of evidence apply than in the political process of naming and shaming. Evidence must stand up in court, making intelligence sources of limited use. Accordingly, the processes of political and legal attribution do not necessarily run in sync and sometimes there is a lack of consistency between them. For example, in the early stages after a cyberattack, when uncertainty is high and evidence is still thin, an actor may be falsely held publicly responsible, only for it to be discovered at a later stage, in the course of legal attribution, that this was a false-flag operation. One example of this is the cyberattack on the French broadcaster *TV5 Monde in* 2015, which was initially attributed to Islamic State

22 For an account of the German interpretation of international law, see: The Federal Government, *On the Application of International Law in Cyberspace. Position Paper* (Berlin, March 2021), 12, https://www.auswaertiges-amt.de/blob/2446304/2ae17233b62966a4b7f16d50ca3c6802/on-the-application-of-international-law-in-cyberspace-data.pdf (accessed 6 May 2021).

23 International Law Commission (ILC), *Draft Articles on the Responsibility of States for Internationally Wrongful Acts (ARS)* (August 2001), https://legal.un.org/ilc/texts/instruments/english/commentaries/9_6_2001.pdf (accessed 15 June 2021).

Table1

Criteria for the legal attribution of cyber incidents

Criterion	Required characteristics
Cyberattack (Art. 1(3) and (7) Regulation [EU] 2019/796)	**Actions that involve** **a. access to information systems;** **b. information system interference;** **c. data interference; or** **d. data interception** where such actions are not duly authorised by the owner or by another right holder of the system or data or of part of it, or are not permitted under the law of the Union or the Member State concerned. Including **attempted** cyberattacks
Attacker determination (Art. 1(2) and (4) Regulation [EU] 2019/796)	**Attackers** a. are located outside the EU (natural/legal persons, entities or bodies) or operate from outside the EU; b. use infrastructure outside the EU. **Victims** within the EU (critical infrastructures, including submarine cables and objects launched into outer space as part of critical infrastructure).
Damage and scope (Art. 2 Regulation [EU] 2019/796)	Determination of "significant effect" is measured according to a. the **scope, extent, effect or severity of disruption caused, including to** economic and societal activities, essential services, critical state functions, public order or public safety; b. the number of natural or legal persons, entities or bodies affected; c. the number of **Member States** concerned; d. the **amount of economic loss** caused, such as through large-scale theft of funds, economic resources or intellectual property; e. the **economic benefit** gained by the perpetrator for himself or for others; f. the **amount or nature of data stolen** or the scale of data breaches; or g. the nature of commercially sensitive data accessed.

Table 1 (continued)

Criteria for the legal attribution of cyber incidents

Criterion	Required features
Target or victim (Art. 1(4) Regulation [EU] 2019/796)	a. **Critical infrastructure**, including **submarine cables** and objects launched into **space**, which is essential for the maintenance of vital functions of society or the health, safety, security and people's economic or social well-being; b. **Services** necessary for the maintenance of essential social and/or economic activities, in particular in the following sectors: 1. Energy (electricity, oil and gas) 2. Transport (air, rail, water and road) 3. Banking, financial market infrastructures 4. Healthcare (healthcare providers, hospitals and private clinics) 5. Drinking water supply and distribution 6. Digital infrastructure 7. Any other sectors essential for the Member State concerned; c. **Critical state functions**, particularly in the following areas: 1. Defence 2. Governance 3. Functioning of institutions, including those required for public elections or the voting process 4. Functioning of economic and civil infrastructure 5. Internal security 6. External relations, including diplomatic missions d. Storage or processing of classified information e. Government emergency response teams

Source: Own representation

(IS) in the context of terrorist attacks, but was later classified as a Russian false flag operation.[24]

The executive and judiciary may come to different conclusions in classifying the same incident. An actor may be declared responsible because it seems politically convenient, while the technical and legal evidence tells a different story ("politicisation of intelligence"). Considering all these imponderables, it becomes clear how essential it is to develop a common understanding of what is meant by a serious cyberattack. This is a significant challenge for EU cyber diplomacy. The close coordination of attributing organisations at the state level (intelligence services, law enforcement agencies) as well as at

24 Gordon Corera, "How France's TV5 Was Almost Destroyed by 'Russian Hackers'", *BBC News* (online), 10 October 2016, https://www.bbc.com/news/technology-37590375 (accessed 14 July 2021).

the supranational and intergovernmental level is therefore essential.

What is a serious cyberattack against the EU?

In its regulation of 17 May 2019 (Article 1(1) of the Regulation), the EU defines a serious cyberattack as an external threat to the Union or its Member States with a significant or potentially significant impact.[25] An external threat to the Member States occurs if cyberattacks are carried out against critical infrastructures, services or state institutions and processes that are essential for maintaining important societal functions or the health, safety and welfare of the population, in particular in the areas of energy, transport, banking, healthcare, drinking water supply or digital infrastructure (Article 1(4) of the Regulation). A cyberattack (or an attempted cyberattack) describes any act involving access to or interference with information and communication systems. Information systems are systems for the automatic processing of digital data; such a system is classified as having been interfered with if its operation is hindered or disrupted by damage, deletion, alteration, suppression or transmission of digital data. However, cyberattacks also occur when data is interfered with or intercepted. Therefore, stealing data, funds, economic resources or intellectual property, for example, are also classified as cyberattacks (Article 1(3) and (7) of the Regulation). Whether a cyberattack has a (potentially) significant impact is determined, among other things, by the scope, extent, effect or severity of the (attempted) disruption of economic and social activities, by the amount of material damage and the economic benefit obtained by the perpetrator, as well as by the amount and type of stolen data accessed (Article 2 of the Regulation).

Table 1 (p. 12f.) provides an overview of the legal characteristics used to classify cyberattacks. With these factual characteristics, the EU defines prohibited conduct and determines which characteristics a cyber incident must fulfil under EU law in order to trigger a specific legal consequence.

Which institutions and procedures determine attribution?

The general principle of law (General Principle, Art. 38 para. 1c ICJ Statute) states that every state has the obligation not to knowingly permit its territory to be used for acts that violate the rights of other states.[26] Under these principles, each Member State is free to choose its own method and procedure for attribution. While political attribution remains a sovereign act of the Member States, at the same time the EU has an essential coordinating function. There is no clear hierarchy in the "chain of command".[27] Institutionally, attribution is thus a parallel process running between the Commission, the Council and Europol and in coordination with the 27 Member States (see Figure 2, p. 15).

The Commission has set out the principles of EU action that also guide the other EU institutions. In September 2017, it prepared a *blueprint* for a coordinated response to large-scale cross-border cybersecurity incidents (*blueprint* for short).[28] The guiding principles

25 Council of the European Union, "Council Regulation (EU) 2019/796 of 17 May 2019 concerning restrictive measures against cyber-attacks threatening the Union or its Member States", *Official Journal of the European Union*, no. L 129 I/1 (17 May 2019), https://eur-lex.europa.eu/legal-content/GA/TXT/?uri=CELEX%3A32019R0796 (accessed 2 June 2021).

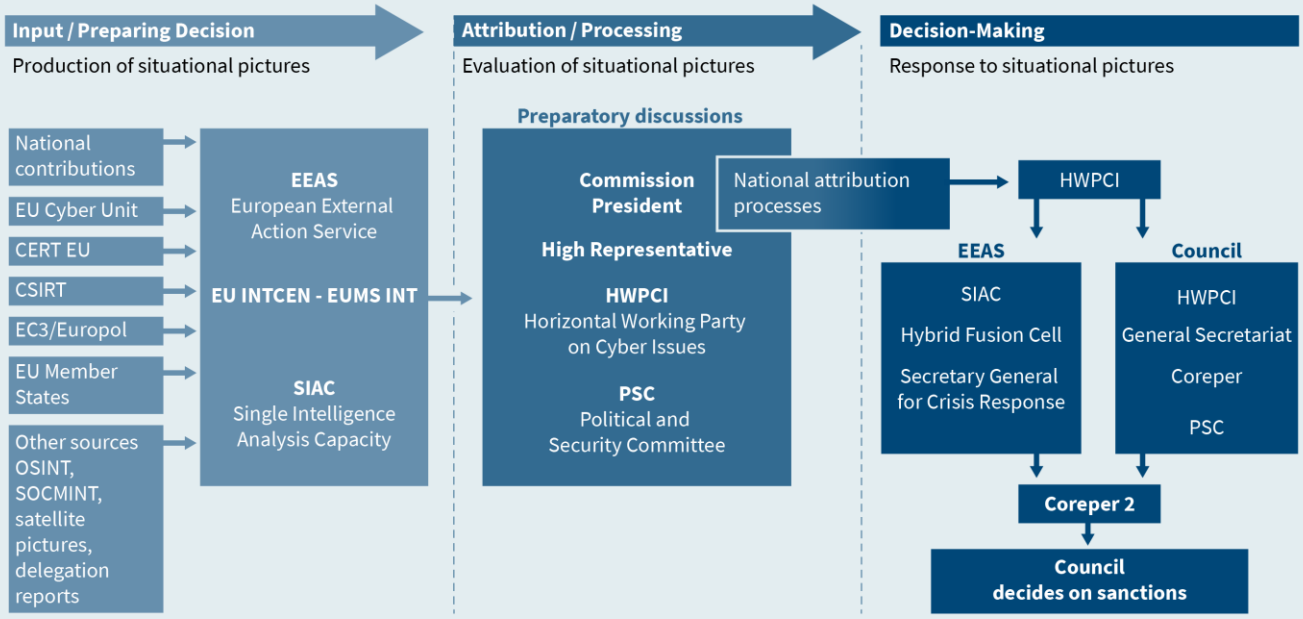
26 "Island of Palmas Case (Netherlands, USA), 4 April 1928", in *Reports of International Arbitral Awards*, ed. United Nations, vol. II (Lake Success, 1949), 829–71 (839); International Court of Justice (ICJ), *The Corfu Channel Case. Judgment of 9 April 1949*, ICJ Reports 1949 (The Hague, February 1949), 22, and ICJ, *Case Concerning Pulp Mills on the River Uruguay (Argentina v. Uruguay). Judgment of 20 April* 2010, ICJ Reports 2010 (The Hague, 2010), p. 69, para. 197: "obligation to act with due diligence in respect of all activities which simply take place under the jurisdiction and control of each party", https://www.icj-cij.org/public/files/case-related/135/135-20100420-JUD-01-00-EN.pdf (accessed 14 September 2021); see also Michael N. Schmitt, ed. *Tallinn Manual on the International Law Applicable to Cyberwarfare* (Cambridge: Cambridge University Press, 2013), 27–8, para. 8.

27 Council of the European Union, "Regulation (EU) 2019/796" (see note 25).

28 European Commission, "Commission Recommendation (EU) 2017/1584 of 13 September 2017 on Coordinated Response to Large-scale Cybersecurity Incidents and Crises", *Official Journal of the European Union*, no. L 239 (19 September 2017): 36–58, https://eur-lex.europa.eu/eli/reco/2017/1584/oj; Council of the European Union, *EU Coordinated Response to Large-Scale Cybersecurity Incidents and Crises – Council Conclusions* (Brussels, 26 June 2018), https://data.consilium.europa.eu/

Figure 2

Cyber Diplomacy Toolbox
EU cyber diplomatic response framework



are respect for proportionality, subsidiarity, complementarity and confidentiality of information in the policy response to cyberattacks.[29] In its draft, the EU Commission focused on building a resilient ICT structure, protecting the single market and implementing a cyber crisis response process. This so-called blueprint mechanism and the creation of the Joint Cyber Unit run in parallel to the CFSP's crisis management. Diverging institutional interests may well exacerbate existing contradictions and incoherencies, but it is already becoming apparent that the EEAS, the Hybrid Fusion Cell within the EU INTCEN, has grown into its role. Member States realise that sharing information on cyber incidents provides collective added value. The EEAS shares information on the cyber warfare doctrines of third countries.

The framework for a joint diplomatic response to malicious cyber activities, the diplomatic response framework, takes effect when the Council has agreed that an external threat exists (see Figure 2, p. 15). Each Member State can submit a proposal to activate a specific measure or escalatory step from the repertoire of the cyber diplomacy toolbox. The preparatory arrangements for the Council decision are made by the Political and Security Committee (PSC), the Horizontal Working Party on Cyber Issues (HWPCI or HWP Cyber), the Commission President and her deputies, as well as the High Representative for Foreign Affairs and Security Policy (see Figure 2, centre). Cyberattacks are discussed and managed in the Horizontal Working Group, the technical body within the EU which coordinates the actions of the EU Member States. The Group receives evidence, which is investigated and verified by the law enforcement agencies and intelligence services of the Member States, in cooperation with the Computer Security Incident Response Teams (CSIRTs), the European Cybercrime Centre (EC3), the European Union Agency for Cybersecurity (ENISA) or the EU Computer Emergency Response Team (CERT-EU) (see Figure 2, top right).

The EEAS pools the collected information (Figure 2, left). Here, the responsibility lies with the Deputy Sec-

doc/document/ST-10086-2018-INIT/en/pdf (accessed 2 June 2021).

29 Along with the Joint Cyber Unit of the European Commission, the relevant institutions, bodies and agencies of the EU Member States are to collaborate through a European platform. Under the Network and Information Security (NIS) Directive, Computer Security Incident Response Teams (CSIRTs) are already expected to share their technical solutions.

retary-General for Crisis Response, the Single Intelligence Analysis Capacity (SIAC, which in turn consists of representatives from EU INTCEN and the Intelligence Division of the EU Military Staff, EUMS INT), and the Hybrid Threat Analysis Unit (EU Hybrid Fusion Cell).[30] The focal point for a coordinated response is Europol's European Cybercrime Centre (EC3). Serious cyber incidents should be reported to Europol. The EU's top police authority conclusively identifies, assesses and classifies cyber incidents according to a threat matrix.[31] Information for the assessment of the threat and damage potential is gathered via the Member States.

In the Council, the Council Presidency (which is also the chair of the Horizontal Working Party on Cyber Issues [HWPCI]) or the Permanent Representatives Committee (Coreper) deals with cybersecurity incidents. It is supported by the General Secretariat of the Council or the Political and Security Committee (PSC, chart 2, centre right). At the working level, HWP Cyber is the central authority for attribution.[32] It is here, in particular with the help of the legal department, that the factual legal dimension and the reliability of the information is analysed. The latter always requires a query to be submitted to INTCEN/SIAC. The classification of a cyber incident follows a linguistically defined code (probability yardstick). The Member States use a comparable standardised system just to be able to classify statements that have not been proven forensically. For the HWP Cyber, the goal of political attribution is to arrive at a common situation awareness. The willingness of Member States to participate in this process has increased with the increase in the number of publicly available forensic indicators of compromise (IoC). These are often documented by private security analysis firms and are widely available.

Comprehensive intelligence, publicly available information, including information on the possible motivations of the attacker, but also technical indicators are key evidence to be able to issue cyber sanctions. The evidence may also be fundamental for investigations in criminal proceedings.[33] At EU level, the Committee of Permanent Representatives (Coreper II) will decide on whether further investigations are deemed necessary or whether the Council can impose sanctions. According to Article 31(1) of the Treaty on European Union (TEU), decisions must be taken by the Council acting unanimously. The natural or legal persons, entities or bodies responsible may then be included in the implementing regulation, i.e. placed on the sanctions list.[34] A Council decision on the CFSP is a non-legislative act, but the Council's implementing decisions and regulations are binding under Article 28(2) TEU on cyber sanctions.[35]

The cyber diplomacy toolbox: A step-by-step plan

The European Council or the Foreign Affairs Council agrees on the attribution and is responsible for the response to cyberattacks. The repertoire of measures in the cyber diplomacy toolbox largely coincides with the classic CFSP toolbox. However, the former is designed as a concrete step-by-step plan with increasing escalation potential. The attribution of a cyberattack to an originator is a necessary precondition for this. Each individual escalation level with the corresponding reaction, whether that be diplomatic, political or in compliance with international law, requires a unanimous Council decision (see Table 2, p. 18).

30 Investigations in criminal proceedings in cases of cyberattacks are carried out by the national law enforcement authorities. They are supported by Europol and the Joint Cybercrime Action Taskforce (JCAT) at the European Cybercrime Centre (EC3).

31 Since 2018, the EU has been using the EU Law Enforcement Emergency Response Protocol (EU LE ERP) under the auspices of Europol.

32 Council of the European Union, "Council Implementing Decision (EU) 2018/1993 of 11 December 2018 on the EU Integrated Political Crisis Response Arrangements", *Official Journal of the European Union*, no. L 320/28 (17 December 2018), https://eur-lex.europa.eu/eli/dec_impl/2018/1993/oj (accessed 2 June 2021). Cybersecurity is also to be included in the "Integrated Political Crisis Response" (IPCR) at Council level.

33 Council of the European Union, *Draft Implementing Guidelines for the Framework on a Joint EU Diplomatic Response to Malicious Cyber Activities* (9 October 2017), https://data.consilium.europa.eu/doc/document/ST-13007-2017-INIT/en/pdf (accessed 2 June 2021).

34 Matthias Monroy, "EU beschließt System für Cyber-Sanktionen", *Telepolis*, 20 May 2019, https://www.heise.de/tp/features/EU-beschliesst-System-fuer-Cyber-Sanktionen-4426777.html (accessed 7 June 2021). The sanctions will be implemented by the Member States in accordance with the 2017 version of the Common Foreign and Security Policy of the EU (Document 15579/03).

35 See Art. 24 para. 1 sentence 3 TEU in conjunction with Art. 31 para. 1 subparagraph 1 sentence 2.

A wide range of CFSP tools can be used in cyber diplomacy.

The CFSP instruments used in cyber diplomacy range from preventive, cooperative, stabilising and restrictive measures to punitive measures for self-defence in accordance with international law. The intensity and scope of possible responses to cyber-attacks increases accordingly.[36] The EU Cyber Diplomacy Toolbox and the cyber sanctions therefore fulfil a "signalling" and "naming and shaming" function. The EU's expected diplomatic counterreaction is thus transparent for each level of escalation.[37] Potential attackers are to be deterred from malicious acts by the threat of legal, economic and military sanctions: "Sanctions are one of the options available in the Union's framework for a joint diplomatic response to malicious cyber activities (the so-called *cyber diplomacy toolbox*) and are intended to *prevent*, *discourage, deter and respond* to *continuing and increasing malicious behaviour in cyberspace*".[38]

Thus, depending on the severity of a cyber incident, a tailor-made diplomatic and/or appropriate response in conformity with international law can be taken from the toolbox. While the preventive and cooperative measures are largely similar to the classic instruments of diplomatic mediation, the stabilising and restrictive measures are aimed at concrete prevention of threats. The response in accordance with international law is decided autonomously by the EU heads of state and government.

This classification helps to make EU action more predictable and thus more reliable for third parties.

Preventive measures are low intensity and do not necessarily require attribution. This category includes formats for political dialogue with third countries. These are designed to influence the behaviour and position of partners by exchanging information and deepening cooperation.

Cooperative measures include, for example, EU demarches, i.e. diplomatic protest notes that can be submitted by the EU delegation in the respective host country on the instructions of the High Representative (HR). Demarches can also be made jointly with third countries.

Stabilising measures: The Council unanimously agrees on an EU action or common position. Implementing stabilising measures requires a unanimous decision. However, Article 31(2) TEU allows decisions to be made based on a qualified majority, unless the measures have military or defence implications. This could open up the possibility for appropriate decisions in the field of cyber diplomacy. So far, this option has not been used, however. A weaker signal can be sent by the HR on behalf of the EU by issuing a declaration for which the Council must give its prior consent. A declaration by the HR "on behalf of the EU" is usually made in cases where an EU position needs to be developed in light of a new situation or where an existing position needs to be adapted. However, the HR may also issue a declaration on its own responsibility if a rapid reaction is required and coordination within the EU 27 is not possible. However, in international diplomacy, other states usually notice whether or not all EU members have agreed to a declaration.

Restrictive measures: The EU may impose restrictive measures to enforce policy objectives resulting from serious cyberattacks. Such sanctions currently represent the highest level of escalation below the threshold of an armed conflict. They are, so to speak, the "hammer" in the EU toolbox (and are also referred to as such), as they are designed to have painful economic effects on third-party actors. Restrictive measures are usually directed against representatives of governments of certain third countries, but also against state-owned companies or other legal and natural persons. They must be adopted unanimously by the Council and be in line with the objectives of the CFSP as set out in Article 24 TEU.

36 Annegret Bendiek, *The EU as a Force for Peace in International Cyber Diplomacy*, SWP Comment 19/2018 (Berlin: Stiftung Wissenschaft und Politik, April 2018), https://www.swp-berlin.org/publikation/the-eu-as-a-force-for-peace-in-international-cyber-diplomacy.

37 See James D. Fearon, "Signaling Foreign Policy Interests", *Journal of Conflict Resolution* 41, no. 1 (1997): 68–90; Florian J. Egloff and Myriam Dunn Cavelty, "Attribution and Knowledge Creation Assemblages in Cybersecurity Politics", *Journal of Cybersecurity* 7, no. 1 (2021), doi: 10.1093/cybsec/tyab002.

38 Council of the European Union, "Malicious Cyber-attacks: EU Sanctions Two Individuals and One Body over 2015 Bundestag Hack", press release, 22 October 2020 (emphasis in original), https://www.consilium.europa.eu/en/press/press-releases/2020/10/22/malicious-cyber-attacks-eu-sanctions-two-individuals-and-one-body-over-2015-bundestag-hack/ (accessed 14 September 2021).

Table 2

EU cyber diplomacy response framework (cyber diplomacy toolbox), extracted from: see Source

Preventive measures	Cooperative measures	Stabilising measures	Restrictive measures	Measures in conformity with international law
■ Confidence and security-building dialogues ■ Capacity building in third countries ■ Awareness raising	■ EU demarches (if necessary in cooperation with third countries) ■ Diplomatic protest notes	■ Common Position of the European Council ■ CFSP ■ Decision ■ Statements by HR on behalf of the Council ■ Declaration of HR	■ Measures under Art. 215 TFEU/CFSP Decision Title V Chapter 2 TEU ■ Account blocking ■ Travel restrictions	■ Solidarity clause (Art. 222 TFEU) ■ Assistance clause (Art. 42 (7) TEU) in accordance with Article 51 UN Charter (right of self-defence)

Resilience	Defence (Denial)		Retaliation
	Examples:	**Examples:**	
	■ (Non-public) Demarche "on the need to respect the rules-based order in cyberspace" (April 2019) ■ (Non-public) Demarche "on the need to respect the rules-based order in cyberspace" (November 2019)	■ Council conclusions on WannaCry and NotPetya (April 2018) ■ "Common messages" (2018) ■ Statement HR/VP, Presidents of the European Council and the EU Commission on the OPCW attack (October 2018) ■ Declaration by HR on behalf of the EU "to respect the rules-based order in cyberspace" (April 2019).	■ Horizontal cyber sanctions regime (May 2019). ■ "Coordinated Attribution at EU Level" (Annex to the Implementation Guidelines, June 2019). ■ Council Regulations (July 2020)

Sources: Council of the European Union, *Draft Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities ("Cyber Diplomacy Toolbox") – Adoption* (Brussels, 7 June 2017), and Council of the European Union, *Draft Implementing Guidelines for the Framework on a Joint EU Diplomatic Response to Malicious Cyber Activities* (Brussels, 9 October 2017).

In the EU, as a general rule, sanctions should always be targeted (targeted sanctions).[39] Broad trade embargoes have proven to be ineffective in the past and might harm civil society. Therefore, the EU generally imposes targeted measures such as asset freezes

39 Council of the European Union, *Sanctions: How and When the EU Adopts Restrictive Measures*, 13 July 2021, https://www.consilium.europa.eu/en/policies/sanctions/ (accessed 13 July 2021).

and travel and investment bans in response to malicious activities in the cyber and information space.[40] Lists of individuals and companies, asset freezes or entry restrictions apply in all Member States. In principle, the persons targeted have the possibility of taking legal action against the imposition of sanctions. Legal protection against being listed by means of an implementing regulation exists via an action for annulment pursuant to Article 263 IV TFEU before the European Court of Justice (ECJ).

Restrictive measures under the CFSP are the most invasive instrument available in the cyber diplomacy toolbox below the threshold of an armed conflict. However, there is a sizable gap in the toolbox between the means available for civilian conflict resolution and those available for military conflict resolution as the highest level of escalation.

Responding in accordance with international law: The application of the solidarity and mutual assistance clauses, which only became part of the EU acquis with the Lisbon Treaty, is also an option in the event of a serious cyberattack against a Member State or the EU as a whole. The solidarity clause under Article 222 TFEU provides for EU states to assist each other if one or more of them has been the victim of terrorist attacks, natural or man-made disasters — and thus also of serious cyber incidents.

The strongest means of reaction would be to activate the mutual assistance clause under Article 42(7) TEU. The provision roughly corresponds to Article 5 of the NATO Treaty, but is subsidiary to it for NATO members. Specifically, it means that "in the event of an armed attack on the territory of a Member State", the other Member States must provide assistance in accordance with Article 51 of the UN Charter (right of self-defence).[41] Both clauses can only be applied in the case of cyberattacks, which constitute a violation of the prohibition of the use of force (Art. 2.4 UN Charter) as *jus cogens.*

However, the right to military self-defence against cyberattacks is accompanied by high requirements: On the one hand, a cyber operation must be comparable to the use of armed force in terms of scope and effect in order to be classified as such. In addition, the operation must be either directly or indirectly attributable to a state or it must be possible to prove its responsibility (in a court of law).

Only a small number of Member States are technically capable of reactive defensive cyber counterattacks or cyber operations of their own.

Cyber sanctions need not necessarily be limited to the conventional instruments of the Common Foreign and Security Policy or the EU's Common Security and Defence Policy described above. Self-defence can also take place within the cyber and information domain space.[42] As a last resort in the toolbox, the heads of state and government in the Council have the possibility to decide on an "active" cyber defence in the form of a digital retaliatory strike ("hack back"). Reactive defensive cyber counterattacks or own cyber operations in third countries are possible under certain conditions, for example for security purposes. Currently, however, only a small number of Member States have the technical capabilities to execute these. Cyber operations on foreign networks in peacetime may constitute a violation of sovereignty. There is always the risk of causing significant collateral damage to innocent third parties. This, too, is at odds with the EU's cyber strategy, which focuses on conflict prevention instead of escalation, on mitigating rather than exploiting IT insecurities, and on confidence and security-building measures and cyber diplomacy legitimised by the rule of law and international law.[43]

40 Patryk Pawlak and Thomas Biersteker, *Guardian of the Galaxy. EU Cyber Sanctions and Norms in Cyberspace*, Chaillot Paper 155 (Paris: European Institute for Security Studies, October 2019), 9, https://www.iss.europa.eu/content/guardian-galaxy-eu-cyber-sanctions-and-norms-cyberspace (accessed 6 May 2021).

41 "Consolidated Version of the Treaty on European Union", *Official Journal of the European Union*, 26 October 2012, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A12012M%2FTXT (accessed 12 November 2021).

42 Council of the European Union, *Sanctions* (see note 39).

43 Jack Goldsmith and Alex Loomis, *"Defend Forward" and Sovereignty*, Aegis Series Paper no. 2102 (Stanford, CA: Hoover Institution, April 2021), https://www.hoover.org/sites/default/files/research/docs/goldsmith-loomis_webreadypdf.pdf; Jason Healey, "Memo to POTUS: Responding to Cyber Attacks and PPD-20", *The Cipher Brief*, 24 May 2018, https://www.thecipherbrief.com/column_article/memo-potus-responding-cyber-attacks-ppd-20.

Case Studies: EU Cyber Sanctions and Their Attribution

The cyberattacks WannaCry 2017, NotPetya 2017, Operation Cloud Hopper 2017, Bundestag hack 2015 and the attempted attack on the Organisation for the Prohibition of Chemical Weapons (OPCW) 2018 formed the basis for the imposition of the first EU cyber sanction regime by the Council of the European Union in July 2020. The Council had already classified these cases as malicious cyberattacks with a significant impact on the security of the Union and its Member States in May 2019.[44] The European Commission and the High Representative justified the adoption of cyber sanctions on the basis of a hybrid threat constellation to the Union.[45] The aforementioned cases are examined below with the aim of understanding the technical, political and legal dimensions of the EU's attribution process. The analysis conducted is based on the elements defined in Council Regulation (EU) 2019/796 and Council Decision (CFSP) 2019/797 (see above, Table 1, p. 12).[46] In the following, the discrepancies between a legally necessary and a politically sufficient attribution are illustrated on the basis of the first cyber sanctions regime and the cyber incidents on which it is founded.

WannaCry 2017

The WannaCry cyberattack began on 12 May 2017 and lasted only a few days. WannaCry was a type of ransomware. Ransomware encrypts target systems and renders them unavailable. Data is not available to the user until the ransom is paid, usually in bitcoins.[47] The malware spread independently, much like a worm, on vulnerable target systems.[48] This infection technique was based on a cyberattack exploit previously stolen from the U.S. National Security Agency (NSA) called EternalBlue. The same vulnerability was also used in the NotPetya attack and in Chinese APT (advanced persistent threat) campaigns.[49] EternalBlue used a flawed implementation of Microsoft's SMB protocol to access files and printers on

44 Council of the European Union, "Regulation (EU) 2019/796" (see note 25), Art. 2.

45 European Commission, High Representative of the Union for Foreign Affairs and Security Policy, *Joint Communication to the European Parliament and the Council: Joint Framework on countering hybrid threats – a European Union response*, Brussels, 6 April 2016 (JOIN/2016/18 final), https://eur-lex.europa.eu/legal-content/DE/ALL/?uri=CELEX%3A52016JC0018 (accessed 2 June 2021).

46 Council of the European Union, "*Council Decision (CFSP) 2019/797 of 17 May 2019 Amending Decision (CFSP) 2019/797 Concerning Restrictive Measures against Cyber-attacks Threatening the Union or Its Member States*", *Official Journal of the European Union*, no. L 129 I/13 (17 May 2019), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32021D0796&from=DE (accessed 2 June 2021); idem, "Regulation (EU) 2019/796" (see note 25).

47 In this case, reports on whether data was released after the ransom was paid are conflicting; Brian Krebs, "Global 'Wana' Ransomware Outbreak Earned Perpetrators $26,000 so Far", *Krebs on Security*, 13 May 2017, https://krebsonsecurity.com/2017/05/global-wana-ransomware-outbreak-earned-perpetrators-26000-so-far/ (accessed 2 June 2021).

48 Zammis Clark, "The Worm That Spreads WanaCrypt0r", *Malwarebytes*, 12 May 2017, https://blog.malwarebytes.com/threat-analysis/2017/05/the-worm-that-spreads-wanacrypt0r/; Austin McBride, "The Hours of WannaCry", *Cisco Umbrella* (online), 16 May 2017, https://umbrella.cisco.com/blog/the-hours-of-wannacry (both accessed 2 June 2021).

49 Andy Greenberg, "The Strange Journey of an NSA Zero-Day — Into Multiple Enemies 'Hands'", *Wired* (online), 7 May 2019, https://www.wired.com/story/nsa-zero-day-symantec-buckeye-china/ (accessed 2 June 2021).

other machines on the same network. This allowed the malware to jump from computer to computer with no user interaction. This remained the case as long as Microsoft was unable to close the vulnerabilities in its Windows operating system with patches.[50]

Victims, damages and aim of the operation

According to media reports, approximately 230,000 computers in around 150 countries were affected by the WannaCry attack, including EU Member States. The wormable nature of WannaCry allowed it to spread uncontrollably, resulting in numerous collateral effects. Ransom payments of around US$35,000 were made to decrypt the data. The total damage was estimated at around four billion U.S. dollars.[51] Victims of the attack included companies such as Télefonica and O_2 (Spain and EU), DB Schenker (a subsidiary of Deutsche Bahn), FedEX (USA), Renault (France), Nissan in the UK, Sony Pictures (USA), telecommunications companies Vivo (Brazil) and MegaFon (Russia), Sandvik (Sweden), PetroChina and Chinese gas stations. Banco Bilbao Vizcaya Argentaria (Spain), Bangladesh Bank, Tien Phong Bank (Vietnam),[52] the Russian Ministry of Internal Affairs, the Romanian Ministry of Foreign Affairs and the Polish Financial Supervisory Authority were also affected.[53] The UK National Health Service (NHS) and numerous British hospitals had to suspend their operations.[54] The damage in the UK was estimated at around £92 million. More than 19,000 treatments had to be cancelled. The attack therefore had an impact on the health and lives of patients.[55] Deutsche Bahn's ticket machines failed and blackmail messages appeared on numerous display boards.[56]

The strategic goal of the operation is somewhat difficult to determine. The nature of the worm, the use of an NSA exploit, the built-in "kill switch" via a domain name that can be extracted from the malicious code, and the need to manually decrypt infected computers all suggest that WannaCry was intended as a minor disruption and to create conflict with the NSA. The fact that the attack was relatively amateur is inconsistent with a professional ransomware campaign and suggests that the motivation was not criminal: "High damage, high publicity, very high visibility to law enforcement, and probably the lowest profit margin we've seen from moderate or even small ransomware campaigns", said cybersecurity researcher Craig Williams in his analysis of the attack.[57] There were also suspicions that the attack could have been a red herring to cover up other espionage operations or expose NSA operations. WannaCry could also have been a "last resort effort", i.e. a measure aimed at capitalising on a previously exposed cyber operation before the vulnerability became useless.[58]

Attribution of the attackers

In June 2017, just two months after WannaCry, the NSA and the UK's Government Communications Headquarters (GCHQ) intelligence agency claimed, with "moderate certainty", that North Korea's "Reconnaissance General Bureau" was linked to the WannaCry

50 Alex Berry, Josh Homan and Randy Eitzman, "WannaCry Malware Profile", *FireEye*, 23 May 2017, https://www.fireeye.com/blog/threat-research/2017/05/wannacry-malware-profile.html (accessed 2 June 2021).

51 Christof Windeck, "WannaCry: Gewaltiger Schaden, geringer Erlös", *Heise Online*, 14 May 2017, https://www.heise.de/security/meldung/WannaCry-Gewaltiger-Schaden-geringer-Erloes-3713689.html (accessed 2 June 2021).

52 Volker Briegleb, "Ransomware WannaCry befällt Rechner der Deutschen Bahn", *Heise Online*, 13 May 2017, https://www.heise.de/newsticker/meldung/Ransomware-WannaCry-befaellt-Rechner-der-Deutschen-Bahn-3713426.html; Stefan Betschon, "Wanna Cry: Bilanz des Hackerangriffs in 150 Ländern", *Neue Zürcher Zeitung* (online), 15 May 2017, https://www.nzz.ch/international/computersicherheit-cyberangriff-gefaehrdet-windows-pc-rund-um-die-welt-ld.1293201 (all accessed 2 June 2021).

53 Bundeskriminalamt, *Cybercrime. Bundeslagebild 2017* (Wiesbaden, July 2018), https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrimeBundeslagebild2017.html (accessed 2 June 2021).

54 "NHS Services Still Facing Cyber Threat", *BBC News* (online), 15 May 2017, https://www.bbc.com/news/uk-39921479 (accessed 2 June 2021).

55 Saira Ghafur et al, "A Retrospective Impact Analysis of the WannaCry Cyberattack on the NHS", *npj Digital Medicine* 2 (2019).

56 Bundeskriminalamt, *Cybercrime. Bundeslagebild 2017* (see note 53), 12.

57 Andy Greenberg, "The WannaCry Ransomware Hackers Made Some Real Amateur Mistakes", *Wired* (online), 15 May 2017, https://www.wired.com/2017/05/wannacry-ransomware-hackers-made-real-amateur-mistakes/ (accessed 2 June 2021).

58 Rafael Amado, "WannaCry: An Analysis of Competing Hypotheses", *Digital Shadows* (online), 18 May 2017, https://www.digitalshadows.com/blog-and-research/wannacry-an-analysis-of-competing-hypotheses/ (accessed 2 June 2021).

cyberattack.[59] The UK and U.S. governments' public attribution of North Korea came six months later on 18 December 2017. The U.S. did not impose sanctions immediately.[60] The UK National Cyber Security Centre (NCSC) said there was a "high probability" that the North Korean group "Lazarus" or "APT 38" was responsible for the attacks. The Five Eyes intelligence alliance (UK, U.S., Australia, New Zealand, Canada) and Japan backed this judgement. The governments involved did not provide any concrete evidence, with the clues instead coming from the cyber security industry. Symantec's Amy L. Johnson had drawn a connection to the APT group Lazarus a few months earlier, in late May 2017.[61] Security researchers Rafael Amado and Pasquale Stirparo, on the other hand, did not suspect that WannaCry had originated in North Korea.[62] Also in May 2017, security firm Symantec had uncovered earlier versions of WannaCry circulating on the Internet, believed to be the result of malware test runs. These had similarities to the Lazarus Group's tools, techniques/tactics and procedures (TTPs).[63] The components of WannaCry seemed to represent an evolution of the 2014 cyber operation against Sony Pictures. The same zip file passwords were used in WannaCry and the Sony hack. This is an indication that the malware was written by the same group.[64] In addition, the campaigns' bitcoin accounts were similar, suggesting the same creator.[65] The IP addresses of the command and control (C2) servers and the use of similar encryption techniques for secure communication also supported the idea that this was the same group of actors. The U.S. government indicted software developers Park Jin Hyok, Jon Chang Hyok and Kim Il, employees of e-commerce firm Chosun Expo about a year later, in September 2018. The company is owned by the North Korean state.[66] Lazarus' TTPs contained references to user accounts, fake online identities (fake online personas), passwords, reused software codes and IP addresses that belonged to or could be attributed to Chosun Expo.[67]

EU response to WannaCry

On 16 April 2018, the Council published its conclusions condemning the malicious use of information and communication technologies in the form of the WannaCry and NotPetya attacks. However, it was not until the end of July 2020, that it imposed punitive economic measures on the Chosun Expo company,[68] through Executive Order 2020/1125.[69] These targeted sanctions ("smart sanctions") involved the freezing of all funds and economic resources owned, held or controlled by the natural or legal persons, entities or bodies. No funds or economic resources were to be made available, directly or indirectly, to the sanctioned persons, entities or bodies.

59 Ellen Nakashima, "The NSA Has Linked the WannaCry Computer Worm to North Korea", *The Washington Post* (online), 14 June 2017, https://wapo.st/3EnCyoP (accessed 2 June 2021).

60 "Cyber-attack: US and UK Blame North Korea for WannaCry", *BBC News* (online), 19 December 2017, https://www.bbc.com/news/world-us-canada-42407488 (accessed 2 June 2021).

61 Amy L. Johnson, "WannaCry: Ransomware Attacks Show Strong Links to Lazarus Group", *Broadcom,* 22 May 2017, https://community.broadcom.com/symantecenterprise/communities/community-home/librarydocuments/viewdocument?DocumentKey=b2b00f1b-e553-47df-920d-f79281a80269 (accessed 2 June 2021).

62 Amado, "WannaCry. An Analysis" (see note 58); Pasquale Stirparo, "Analysis of Competing Hypotheses, WCry and Lazarus (ACH part 2)", *Internet Storm Center*, 31 May 2017, https://isc.sans.edu/forums/diary/Analysis+of+Competing+Hypotheses+WCry+and+Lazarus+ACH+part+2/22470/ (accessed 2 June 2021).

63 Johnson, "WannaCry" (see note 61).

64 Joseph Menn, "Symantec says 'highly likely' North Korea group behind ransomware attacks", *Reuters*, 23 May 2017, https://www.reuters.com/article/us-cyber-attack-northkorea-idUSKBN18I2SH (accessed 2 June 2021).

65 Further details can also be found in the U.S. Justice Department's indictment, United States District Court for the Central District of California, *United States of America v. Park Jin Hyok*, June 2018, https://www.justice.gov/opa/press-release/file/1092091/download (accessed 14 September 2021).

66 Ibid.

67 Catalin Cimpanu, "How US authorities tracked down the North Korean hacker behind WannaCry", *ZDNet* (online), 6 September 2018, https://www.zdnet.com/article/how-us-authorities-tracked-down-the-north-korean-hacker-behind-wannacry/ (accessed 13 May 2021).

68 Article 3(1) and (2) Council Regulation (EU) 2019/796.

69 The legal basis is Article 13 Council Regulation (EU) 2019/796 (in conjunction with Art. 215 TFEU and Art. 21 TEU).

The attribution of responsibility to Lazarus/APT38 was preceded by elaborate diplomatic efforts.

The attribution of responsibility to Lazarus/APT38 was preceded by elaborate diplomatic efforts. The attribution was based predominantly on information from the U.S. security services. The indictment against Park Jin Hyok — according to the U.S. Department of Justice[70] an employee of a shell company in the service of the North Korean government — was based on about 1,000 seized email and social media accounts and 85 international letters. Mandiant and FireEye also played a central role in the attribution process.[71] The criminal complaint against Park Jin Hyok revealed that the person, email addresses, IT infrastructure for the attack, victims and malware families were connected.[72]

Estonia,[73] the Netherlands,[74] France,[75] the UK,[76] Australia[77] and the U.S.[78] also welcomed the EU's restrictive measures as a means of strengthening the message to those responsible. The U.S. attributed the attack to North Korea[79] in June 2017, with the UK[80] following suit in October 2017.[81] While the UN Office on Drugs and Crime, or more specifically its Chief of Cybercrime Neil Walsh, condemned the WannaCry attack as a criminal act, no action was taken under international law.[82]

NotPetya 2017

On the eve of Ukraine's "Constitution Day" (27 June 2017), a wiper malware disabled numerous computers around the world, but especially in Ukraine. It did this by deleting ("wiping") hard drives.[83] The NotPetya malware entered a local network via a supply chain attack on the update mechanism of Ukraine's M.E.Doc tax management software.[84] The malware spread

70 U.S. Department of Justice, *North Korean Regime-Backed Programmer Charged with Conspiracy to Conduct Multiple Cyber Attacks and Intrusions* (Washington, D.C., 6 September2018), https://www.justice.gov/opa/pr/north-korean-regime-backed-programmer-charged-conspiracy-conduct-multiple-cyber-attacks-and (accessed June 2, 2021).

71 U.S. District Court for the Central District of California, *United States of America v. Park Jin Hyok* (see note 65), 2.

72 Ibid., 175.

73 Republic of Estonia, Ministry of Foreign Affairs, "The EU implements its cyber sanctions regime for the first time" (Tallinn, 30 July 2020), https://vm.ee/en/news/eu-implements-its-cyber-sanctions-regime-first-time (accessed 1 October 2021).

74 Government of the Netherlands, "Blok: 'EU condemns malicious behaviour in cyberspace'" (The Hague, 30 July 2020), https://www.government.nl/latest/news/2020/07/30/eu-condemns-malicious-behaviour-cyberspace (accessed 1 October 2021).

75 France Diplomacy, *EU – Cyberattacks – Q&A from the Press Briefing*, 30 July 2020, https://www.diplomatie.gouv.fr/en/french-foreign-policy/digital-diplomacy/france-and-cyber-security/article/eu-cyberattacks-q-a-from-the-press-briefing-30-jul-20 (accessed 1 October 2021).

76 "UK and allies reveal global scale of Chinese cyber campaign", press release, *GOV.UK*, 20 December 2018, https://www.gov.uk/government/news/uk-and-allies-reveal-global-scale-of-chinese-cyber-campaign (accessed 1 October 2021).

77 Australian Government, Department of Foreign Affairs and Trade, *European Union Cyber Sanctions Listings* (1 August 2020), https://www.dfat.gov.au/news/media-release/european-union-cyber-sanctions-listings (accessed 1 October 2021).

78 U.S. Department of State, "The United States Applauds the EU's Action on Cyber Sanctions", Press Statement of Michael R. Pompeo, Secretary of State, 30 July 2020, https://2017-2021.state.gov/the-united-states-applauds-the-eus-action-on-cyber-sanctions/index.html (accessed 1 October 2021).

79 Jack Goldsmith, "The Strange WannaCry Attribution", *Lawfare*, 21 December 2017, https://www.lawfareblog.com/strange-wannacry-attribution (accessed 1 October 2021).

80 "UK and allies reveal global scale of Chinese cyber campaign" (see note 76).

81 The NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), "NotPetya and WannaCry Call for a Joint Response from International Community" (Tallinn, 30 June 2017), https://ccdcoe.org/news/2017/notpetya-and-wannacry-call-for-a-joint-response-from-international-community/ (accessed 1 October 2021).

82 Kolja Brockmann, "European Union sanctions on North Korea: Balancing non-proliferation with the humanitarian impact" (Solna: Stockholm International Peace Research Institute [SIPRI], 11 December 2020), https://www.sipri.org/commentary/topical-backgrounder/2020/european-union-sanctions-north-korea-balancing-non-proliferation-humanitarian-impact, and EU Sanctions Map, updated 21 December 2020, https://bit.ly/2Y8oYWg (both accessed 1 October 2021).

83 Andy Greenberg, "The Untold Story of NotPetya, the Most Devastating Cyberattack in History", *Wired* (online), August 2018, https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/ (accessed 26 May 2020).

84 Jürgen Schmidt, "Petya/NotPetya: Kein Erpressungstrojaner, sondern ein 'Wiper'", *Heise Online*, 29 June 2017, https://www.heise.de/security/meldung/Petya-NotPetya-Kein-

independently, much like a worm, to companies that used the aforementioned software. Companies in numerous states were infected with NotPetya.[85]

So, what did NotPetya do? Once it establishes a bridgehead on a system, a module in the main memory attempts to extract user credentials, including those of administrators with the tool. Using this data, the malware is copied to other computers. The newly infected computer, in turn, triggers the same distribution mechanism. Alternatively, the distribution in corporate networks occurs via the same EternalBlue component that also appeared in WannaCry.[86] Due to similarities in the code, analyses from late June 2017 initially classified the malware as a variant of the Petya ransomware family, which has been used by cyber criminals since 2016,[87] The malware's approach was similar to Petya, encrypting the hard drive and replacing the Microsoft bootloader with a payment request. The attackers demanded a US$300 ransom in bitcoins. In order to recover information, victims were supposed to send an email to an address at the Berlin provider Posteo. The provider immediately blocked the email account.[88]

Victims, damages and aim of the operation

The NotPetya and EternalPetya cyberattacks impacted 65 countries and around 49,000 systems worldwide. Among the victims were numerous companies in the EU.[89] The ransomware resulted in a loss of data availability. The corporations affected included Maersk (Denmark), Rosneft (Russia), Merck Sharp & Dohme (USA), Mondelez (USA), FedEx/TNT (USA/Netherlands), Reckitt Benckiser (UK), Saint-Gobain (France) and Beiersdorf (Germany). In the U.S., the malware crippled the data processing structures of 80 hospitals and medical facilities of the Heritage Valley Health System.[90] The attackers managed to infiltrate Ukrainian IT networks, systems of the National Bank of Ukraine, Kyiv Borispyl International Airport, the capital's metro and the agency for managing the exclusion zone around the damaged nuclear power plant in Chernobyl.[91] Many of the companies affected were essential for the maintenance of services of general interest — including in several EU countries.[92] Worldwide, the cyberattack caused total economic damage of around US$10 billion.[93] Individual companies were unable to restore their IT infrastructures for several weeks. The Danish shipping company Maersk and the freight service provider TNT Express each estimated their losses at over US$300 million. NotPetya is considered one of the most serious and costly cyber incidents.

The operation's objective can be determined quite clearly: certain technical indicators, such as the single contact email address representing a "single point of failure" and allowing the extortion operation to be averted by means of simple countermeasures, are not typical of criminal activity. The unprofessional use of the ransomware raised doubts about whether a state actor was involved. It was only later that the malware's

Erpressungstrojaner-sondern-ein-Wiper-3759293.html (accessed 2 June 2021).

85 Bundeskriminalamt, *Cybercrime. Bundeslagebild 2017* (see note 53), 14.

86 For a detailed description of the bug and exploitation see Nadav Grossman, "EternalBlue — Everything There Is to Know", *Check Point Research*, 29 September 2017, https://research.checkpoint.com/2017/eternalblue-everything-know/; for vulnerability CVE-2017-0144 see *Microsoft security bulletin MS17-010*, 11 October 2017, https://docs.microsoft.com/de-de/security-updates/securitybulletins/2017/ms17-010 (accessed both 14 September 2021).

87 Iain Thomson, "Everything You Need to Know about the Petya, er, NotPetya Nasty Trashing PCs Worldwide", *The Register* (online), 28 June 2017, https://www.theregister.com/2017/06/28/petya_notpetya_ransomware/ (accessed 2 June 2021).

88 Schmidt, "Petya/NotPetya" (see note 84).

89 Jai Vijayan, "3 Years after NotPetya, Many Organizations Still in Danger of Similar Attacks", *Dark Reading* (online), 30 June 2020, https://www.darkreading.com/threat-intelligence/3-years-after-notpetya-many-organizations-still-in-danger-of-similar-attacks/d/d-id/1338200 (accessed 2 June 2021).

90 U.S. Department of Justice, *Six Russian GRU Officers Charged in Connection with Worldwide Deployment of Destructive Malware and Other Disruptive Actions in Cyberspace* (Washington, D.C., 19 October 2020), https://www.justice.gov/opa/pr/six-russian-gru-officers-charged-connection-worldwide-deployment-destructive-malware-and (accessed 2 June 2021).

91 Jonas Jansen and Alexander Armbruster, "Hacker legen Zentralbank und Flughafen in Kiew lahm", *Frankfurter Allgemeine Zeitung* (online), 27 June 2017, https://www.faz.net/aktuell/wirtschaft/ransomware-attacke-legt-viele-unternehmen-lahm-15079944.html (accessed 2 June 2021).

92 Eric Auchard, Jack Stubbs and Alessandra Prentice, "New Computer Virus Spreads from Ukraine to Disrupt World Business", *Reuters*, 27 June 2017, https://www.reuters.com/article/us-cyber-attack-idUSKBN19I1TD (accessed 2 June 2021).

93 Bundeskriminalamt, *Cybercrime. Bundeslagebild 2017* (see note 53), 14.

wiper functionality was discovered, i.e. its ability to cause permanent data loss for those affected. NotPetya disguised itself as standard Petya ransomware. However, the malware was specifically targeted at Ukrainian systems and professionally executed as a political sabotage operation. As the process of attribution progressed, the theory was established that the NotPetya attack was actually a large-scale campaign of destruction targeting Ukraine. This is indicated by the attack vector via software primarily used in Ukraine. Whether the worldwide collateral damage was intended is still unclear; after all, Russian companies were also affected. It is therefore also conceivable that NotPetya was used as a means of diplomatic pressure ("tacit bargaining") against Ukraine due to its high visibility.[94]

Attribution of the attackers

The technical attribution of NotPetya is complicated. The malware is associated with advanced persistent threats (APTs), attack campaigns known in the IT security industry by code names such as "Sandworm", "BlackEnergy group", "Voodoo Bear", "Iron Viking", "Quedagh", "Olympic Destroyer" and "TeleBots". At the time of the incident, it was not known how these APT groups related to each other, whether they were identical or only cooperated selectively, or what relationship they had to state agencies in Russia.

NotPetya part of a multi-year campaign of numerous cyberattacks by these actors against Ukrainian businesses, government agencies and utilities.[95] According to the Slovak IT security firm ESET, the APT group TeleBots used a new backdoor component from April 2018 that had similarities with Industroyer malware frameworks. Industroyer malware had previously been used to attack Ukraine's power grid in December 2016.[96] At that time, the code, attack infrastructure, IoCs and operational target did not allow for a clear political and legal attribution to one actor.[97] Similarities and affinities in the malware of different attack campaigns are only an uncertain indication, as these only point to similar developers, not necessarily the same operational attackers.[98] This is because cybercrime is organised around a division of labour and functionally differentiated, and different groups also copy TTPs.[99] An attack may not be developed and executed by the same group. FireEye provided rather vague arguments for the attribution to Russia, namely that Russian-language documents were found on a C2 server of the APT group and that the group used a zero-day vulnerability in some cyber operations, which had previously been presented at a Russian hacker conference.[100]

The CIA assumes that the Russian military was behind NotPetya. However, no evidence was presented.

The process of political and legal attribution turned out to be a difficult one. The German Federal Criminal Police Office (BKA) had started investigations in 2017, but without issuing an indictment or an arrest warrant. In any case, there was no evidence for either "sufficient" or "urgent suspicion". According to a report in the *Washington Post* in January 2018, the CIA assumed with a "high degree of certainty" that the Russian military (more precisely: the GRU military intelligence service and its main centre for special technologies; GTsST) had been behind NotPetya. No evidence was presented, however.[101] Public attribution occurred in mid-February 2018, with the Five Eyes alliance attributing the attacks to the Russian government.[102] Denmark, Latvia, Sweden and Finland

94 CCDCOE, "NotPetya and WannaCry Call for a Joint Response from International Community" (see note 81).

95 Greenberg, "The Untold Story of NotPetya" (see note 83).

96 Anton Cherepanoy and Robert Lipovsky, "New TeleBots Backdoor: First Evidence Linking Industroyer to NotPetya", *WeLiveSecurity* 11 October 2018, https://www.welivesecurity.com/2018/10/11/new-telebots-backdoor-linking-industroyer-notpetya/ (accessed 2 June 2021). According to ESET, it is unlikely that a third party made the adjustments.

97 See Andy Greenberg, *Sandworm. A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers* (New York: Doubleday, 2019), chap. 36.

98 See ibid, 277.

99 Rolf S. van Wegberg, *Outsourcing Cybercrime* (Delft: Delft University of Technology, 2020), https://doi.org/10.4233/uuid:f02096b5-174c-4888-a0a7-dafd29454450.

100 Andy Greenberg, "Your Guide to Russia's Infrastructure Hacking Teams", *Wired* (online), 12 July 2017, https://www.wired.com/story/russian-hacking-teams-infrastructure/ (accessed 2 June 2021).

101 Ellen Nakashima, "Russian Military Was behind 'NotPetya' Cyberattack in Ukraine, CIA Concludes", *The Washington Post* (online), 13 January 2018, https://wapo.st/3khtQAq (accessed 2 June 2021).

102 Paul Ivan, *Responding to Cyberattacks: Prospects for the EU Cyber Diplomacy Toolbox* (Brussels: European Policy Centre,

declared their support for this attribution. The public attribution enjoyed broad international support.[103] A few months later, in early October 2018, the British NCSC provided more clarity on the question of which APT groups were linked to the GRU. According to the report, these included APT 28, which also operated under the names Fancy Bear and Sofacy. Sandworm, another GRU-affiliated group, is also known as Voodoo Bear and BlackEnergy.[104] The U.S. State Department and the British NCSC did not move to formal legal attribution until February 2020, when they both made references to a similar cyber operation in Georgia for which the aforementioned GRU division GTsST or unit "74455" was declared responsible. The British Foreign Office added apodictically: "This GRU unit [GTsST, 74455] was responsible for [...] NotPetya".[105] The U.S. finally formally indicted six Russian nationals in mid-October 2020.[106] The six officers of the Russian military intelligence agency GRU in military unit 74455 are accused of being involved in several malicious cyberattacks (including the 2015 and 2016 Ukraine blackout attacks, NotPetya, the OPCW cyberattack, and the hack of Emmanuel Macron's campaign team during the 2017 French presidential election).

EU response to NotPetya

On 16 April 2018, the Council of the European Union condemned the malicious use of information and communication technologies, including the cases known as WannaCry and NotPetya.[107] But it was not until two years later, on 30 July 2020, that it issued economic sanctions,[108] in the form of Implementing Regulation (EU) 2020/1125[109] — that is, targeted sanctions against selected individuals.[110] The *Official Journal of the European Union* named the accused actors: "The Main Centre for Special Technologies (GTsST) of the Main Directorate of the General Staff of the Armed Forces of the Russian Federation (GU/GRU), also known by its field post number 74455, is responsible for cyber-attacks with significant impact emanating from outside the Union. It was posing an external threat to the Union and/or its Member States and for third countries. The same threat actor was made responsible for the June 2017 cyber-attacks known as 'NotPetya' or 'EternalPetya' and the cyber-attacks directed against the Ukrainian electricity grid in the winter of 2015 and 2016."[111] The Five Eyes alliance and a small number of EU Member States declared the Russian government responsible much earlier, in February 2018. The EU thus arrived at its collective response more than two years later.

Operation Cloud Hopper 2016

The Cloud Hopper operation is considered a case of industrial espionage.[112] The attack began in 2016 and

March 2019), 5, https://www.epc.eu/content/PDF/2019/pub_9081_responding_cyberattacks.pdf; Francesco Bussoletti, "All Five Eyes countries have blamed Russia for the NotPetya cyber attack", *Difesa & Sicurezza* (online), February 2018, https://www.difesaesicurezza.com/en/cyber-en/all-five-eyes-countries-have-blamed-russia-for-the-notpetya-cyber-attack/ (both accessed 15 September 2021).

103 Ivan, *Responding to Cyberattacks* (see note 102), 5.

104 National Cyber Security Centre, "Reckless Campaign of Cyber Attacks by Russian Military Intelligence Service Exposed" (London, October 2018), https://www.ncsc.gov.uk/pdfs/news/reckless-campaign-cyber-attacks-russian-military-intelligence-service-exposed.pdf (accessed 2 June 2021).

105 Foreign & Commonwealth Office, "UK condemns Russia's GRU over Georgia cyber-attacks", press release, 20 February 2020, https://www.gov.uk/government/news/uk-condemns-russias-gru-over-georgia-cyber-attacks (accessed 2 June 2021).

106 United States District Court for the Western District of Pennsylvania, *United States of America v. Yuriy Sergeyevich Andrienko, Sergey Vladimirovich Detistov, Pavel Valeryevich Frolov, Anatoliy Sergeyevich Kovalev, Artem Valeryevich Ochichenko and Petr Nikolayevich Pliskin,* 15 October 2020, https://www.justice.gov/opa/press-release/file/1328521/download (accessed 15 September 2021).

107 Council of the European Union, "Council Implementing Regulation (EU) 2020/1125 of 30 July 2020 implementing Regulation (EU) 2019/796 concerning restrictive measures against cyber-attacks threatening the Union or its Member States", *Official Journal of the European Union*, no. (30 July 2020) L 246/4, https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32020R1125&from=DE (accessed 2 June 2021).

108 The legal basis for this is Article 13 of Regulation (EU) 2019/796 (in conjunction with Art. 215 TFEU).

109 Ibid., 3rd recital.

110 Council of the European Union, "Council Implementing Regulation (EU) 2020/1125" (see note 107), Annex.

111 Ibid.

112 Lucian Constantin, "'Five Eyes' Countries Attribute APT10 Attacks to Chinese Intelligence Service", *Security Boulevard*, 21 December 2018, https://securityboulevard.com/2018/12/five-eyes-countries-attribute-apt10-attacks-to-chinese-intelligence-service/ (accessed 2 June 2021).

is classified as a supply chain attack. It was directed against what are known as "managed service providers" (MSP). These are companies like Hewlett Packard Enterprise (HPE) and IBM, among others, that provide IT services to third-party companies and government agencies around the world. They manage cloud services, applications and infrastructure such as servers and networks. The hackers penetrated the cloud management infrastructure of these MSPs using "spear phishing" emails disguised as messages from clients of the service providers. According to a technical analysis by Trend Micro, the attackers had installed a modified remote access Trojan (RAT) from the PlugX, Poison Ivy, ChChes and Graftor malware families in Word documents attached to the emails.[113]

The attackers "hopped" (Hopper) across different cloud instances and gained access to the systems.

Once executed, the Trojan established a beachhead on the MSP systems and communicated with C2 servers in Tianjin. It also installed keyloggers that logged and exfiltrated names and passwords for the clients' infrastructure. The hackers used these credentials to laterally access the systems of those same clients via the MSP cloud infrastructure. This modus operandi explains the name Cloud Hopper: The attackers "hopped" over various cloud instances and thus gained access to the systems. The attack is widely considered to be technically adept. The code used certificates from large IT companies to appear authentic. Defending against such supply chain attack vectors is generally considered difficult.[114]

Victims, damages and aim of the operation

According to the *Reuters* news agency, in addition to IBM and HPE, other companies were targeted by the attackers: Ericsson, SKF (both Sweden), Valmet (Finland), Tata Consultancy Services (India), Fujitsu, NTT Data (both Japan), Dimension Data (South Africa), Computer Sciences Corporation, DXC Technology and NASA (all USA).[115] The German Federal Office for Information Security (BSI) issued a warning in December 2018 that German companies could also be affected, but did not specify further.[116] U.S. targets affected were Sabre Corp (USA), a global provider of airline and hotel bookings, and Huntington Ingalls Industries, the largest shipyard in the U.S., which also builds nuclear submarines for the U.S. Navy. 40 U.S. Navy computers were also compromised. The personal information of 100,000 Navy servicemen and women was stolen.[117] A U.S. indictment against the perpetrators mentions at least 25 U.S. entities and 14 other victims in 12 states.[118] Reports on the extent of the damage are conflicting.[119] Compared to other incidents, public information is scarce. The MSP and HPE withheld information about their clients because of liability issues and possible legal consequences. Some companies confirmed successful intrusions but could not determine if data was stolen. There are no estimates of the costs.[120]

There are indications that several teams with different capabilities were working together on the attack.

It is striking that the systems attacked belonged predominantly to the heavy industry sector, aviation and maritime, telecommunications and satellite technology. The operational targets were primarily indus-

113 "Operation Cloud Hopper: What You Need to Know", *Trend Micro,* 10 April 2017, https://www.trendmicro.com/vinfo/pl/security/news/cyber-attacks/operation-cloud-hopper-what-you-need-to-know (accessed 20 May 2021).

114 Jack Stubbs, Joseph Menn and Christopher Bing, "Special Report: Inside the West's Failed Fight against China's 'Cloud Hopper' Hackers", *Reuters*, 26 June 2019, https://www.reuters.com/article/us-china-cyber-cloudhopper-special-repor-idUSKCN1TR1DK (accessed 20 May 2021).

115 Ibid.

116 "German security office warned German firms about Chinese hacking — report", *Reuters*, 19 December 2018, https://www.reuters.com/article/uk-germany-security-idUKKBN1OI0HS (accessed 20 May 2021).

117 U.S. Department of Justice, "Two Chinese Hackers Associated with the Ministry of State Security Charged with Global Computer Intrusion Campaigns Targeting Intellectual Property and Confidential Business Information", press release 18-1673, December 2018, https://www.justice.gov/opa/pr/two-chinese-hackers-associated-ministry-state-security-charged-global-computer-intrusion (accessed 20 May 2021).

118 United States District Court for the Southern District of New York, *United States of America v. Zhu Hua and Zhang Shilong*, Indictment, 20 December 2018, 13ff.

119 Ibid. The DoJ indictment refers to hundreds of gigabytes of stolen intellectual property.

120 IBM Security and Ponemon Institute, *Cost of a Data Breach Report 2019* (Traverse City, MI, 2019), https://www.ibm.com/downloads/cas/ZBZLY7KL (accessed 21 May 2021).

trial espionage or, in the case of Sabre, customer data and, in the case of the Navy, politically motivated intelligence gathering.[121] The attack was difficult to detect and left little trace. There is also evidence that multiple attack teams with different skills divided their efforts, a sign of the complexity of the campaign. The TTPs suggest this was not the typical modus operandi of cybercriminals but more likely a state organisation with substantial financial resources.

Attribution of the attackers

In December 2018, the U.S. government publicly attributed the attack to the group APT 10 (aka menuPass, POTASSIUM, Stone Panda, Red Apollo and CVNX), which is associated with China's Ministry of State Security. The U.S. Department of Justice released the indictments against two Chinese nationals, Zhu Hua and Zhang Shilong.[122] The defendants worked for the Huaying Haitai Science and Technology Development Company in Tianjin, China. Both are said to be part of the APT group, which has specialised in stealing intellectual property from industries in China's strategic interest since 2006. Technical evidence included the malware's communication with IP addresses in Tianjin, the registration of more than 1,300 DNS servers in the U.S., and the congruence of attack activity with office hours in the Chinese time zone. The attribution was based on information from InfraGard and Trend Micro.[123] The Five Eyes alliance concurred with the political attribution. The British NCSC stated that it was "highly likely" that APT 10 had an ongoing relationship with the Chinese Ministry of State Security and was operating under its instructions.[124] Japan, which was also implicated, said it approved of the public attribution.[125] Germany also announced its support for the action a day later.[126]

EU response to Cloud Hopper

In 2019, the EU decided to launch a policy response to the attack under the CFSP. The then High Representative of the Union for Foreign Affairs and Security Policy, Federica Mogherini, declared on 12 April 2019 that malicious cyber activities that undermine the integrity, security and economic competitiveness of the Union and involve intellectual property theft would not be tolerated. The message was directed at the APT 10 group,[127] but it was not until a year later, at the end of July 2020, that the Council went a step further with implementing regulations 2020/1125[128] and 2020/1744,[129] imposing sanctions in November 2020. The travel restrictions, which were one of the measures implemented as a result, are based on Article 4 Decision (CFSP) 2019/797,[130] sanctioning Chinese nationals Gao Qiang and Zhang Shilong, as well as the company Huaying Haitai. They were declared responsible for the cyberattacks between 2014 and 2017.[131] Zhang Shilong was said to be the developer of the malware. Zhang was also said to have been employed by Huaying Haitai, the company that facilitated Operation Cloud Hopper. The timing of the attacks and the targets suggest that the hackers responsible were based in China and had links to the government.[132]

121 Stubbs, Menn and Bing, "Special Report" (see note 114).
122 U.S. Department of Justice, "Two Chinese Hackers" (see note 117).
123 Ibid.
124 Foreign and Commonwealth Office/NCSC, "UK and allies reveal global scale of Chinese cyber campaign" (London, 20 December 2018), https://www.gov.uk/government/news/uk-and-allies-reveal-global-scale-of-chinese-cyber-campaign (accessed 2 June 2021).
125 Constantin, "'Five Eyes' Countries" (see note 112).
126 "Regierungspressekonferenz vom 21. Dezember 2018", *Bundesregierung* (online), 20 May 2021, https://www.bundesregierung.de/breg-de/aktuelles/regierungspressekonferenz-vom-21-dezember-2018-1563932 (accessed 20 May 2021).
127 Council of the European Union, "Declaration by the High Representative on behalf of the EU on respect for the rules-based order in cyberspace", press release, Brussels, 12 April 2019, https://www.consilium.europa.eu/en/press/press-releases/2019/04/12/declaration-by-the-high-representative-on-behalf-of-the-eu-on-respect-for-the-rules-based-order-in-cyberspace/ (accessed 14 September 2021).
128 Council of the European Union, "Implementing Regulation (EU) 2020/1125" (see note 107).
129 Council of the European Union, "Council Implementing Regulation (EU) 2020/1744 of 20 November 2020 Implementing Regulation (EU) 2019/796 concerning restrictive measures against cyber-attacks threatening the Union or its Member States", *Official Journal of the European Union*, no. L 393/1 (23 November 2020), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L%5F.2020.393.01.0001.01.ENG&toc=OJ%3AL%3A2020%3A393%3ATOC (accessed 2 June 2021).
130 Council of the European Union, "Decision (CFSP) 2019/797" (see note 46), Art. 4.
131 Stubbs, Menn and Bing, "Special Report" (see note 114).
132 Federal Bureau of Investigation, "Chinese Hackers Indicted", 20 December 2018, https://www.fbi.gov/news/

Bundestag Hack 2015

It is suspected that on 30 April 2015, an employee of the Left Party (Die Linke) parliamentary group in the German Bundestag opened a link in an email supposedly sent by the UN promising information about the Ukraine conflict.[133] The link led to a compromised website that installed a Trojan. The president of the BSI at the time, Michael Hange, later confirmed to the Bundestag committee that the perpetrators were able to log onto the domain controller and admin workstations on 5 May 2015. Using the tool Mimikatz, they harvested passwords of other user accounts. With the help of extracted passwords and various remote control programs, the attackers gained access to up to 50 additional systems in the Bundestag on 6 May 2015.[134] The intruders gained administrative rights for the Microsoft environment of parliament and parliamentary groups.

On behalf of the Left Party parliamentary group, the independent IT security researcher Claudio Guarnieri gained early access to attack artefacts.[135] He suspected phishing as the means of initial infection, or alternatively a bug in Windows or Flash Player. At that time, it was unclear whether the attack on the Left Party computer was part of the Bundestag hack or an independent attack. The emergency response turned out to be a test of the separation of powers, because the IT security of the legislature had to be supported by the BSI and the Federal Office for the Protection of the Constitution as executive authorities. Years before the domestic intelligence agency, the Office for the Protection of the Constitution, had placed members of the Left Party under surveillance.

Victims, damages and aim of the operation

The Trojan attack compromised the central server of the Bundestag administration and computers of members of parliament, even in the office of Chancellor Angela Merkel. It is believed that a considerable number of email conversations from 2012 to 2015 were stolen.[136] Around 50 IT systems were affected[137] and larger amounts of data were leaked from the Bundestag: "demonstrably" at least 16 gigabytes (possibly with duplicates) were sent "to around nine known, globally distributed, suspicious servers".[138] The exact volume of data and the content of the leaked data (classified information) are not known.[139] By September 2015, the Bundestag's IT department had spent "about €1 million" on incident response. The BSI has had to bill 350 working days for mitigating the damage caused by the cyberattack.[140]

The attack on the highest constitutional body of the Federal Republic of Germany put its democratic functionality at risk. Nevertheless, the aim of the operation was primarily political espionage. In January 2017, unknown persons registered the domain "btleaks.com", presumably with the intention of publishing the stolen data at an opportune moment, for example before the federal elections. This was similar to the hack of the Democratic Party headquarters (DNC hack) in the U.S. in 2016, where the

stories/chinese-hackers-indicted-122018 (accessed 2 June 2021).

133 According to the leaked minutes of the meeting of the relevant Bundestag committee, the president of the BSI said that the initial infection was caused by a so-called watering hole attack; Kommission des Ältestenrates für den Einsatz neuer Informations- und Kommunikationstechniken und -medien [= IuK-Kommission], *Kurzprotokolle der 6., 7. und 8. Sitzung der IuK-Kommission des Deutschen Bundestages,* Berlin, May to July 2015 (non-public and non-official version), https://pastebin.com/raw/LZzpN3Lb (accessed 2 January 2021).

134 "Kurzprotokoll der 7. Sitzung der IuK-Kommission", 11 June 2015, in IuK-Kommission, *Kurzprotokolle* (see note 133).

135 Claudio Guarnieri, "Digital Attack on German Parliament: Investigative Report on the Hack of the Left Party Infrastructure in Bundestag", *Netzpolitik.org*, 19 June 2015, https://netzpolitik.org/2015/digital-attack-on-german-parliament-investigative-report-on-the-hack-of-the-left-party-infrastructure-in-bundestag (accessed 15 September 2021).

136 Jörg Diehl, Marcel Rosenbach and Fidelius Schmid, "Rekonstruktion eines Cyberangriffs: Wie russische Hacker Angela Merkels Mailkonten knackten", *Der Spiegel* (online), 8 May 2020, https://www.spiegel.de/netzwelt/web/angela-merkel-wie-russische-hacker-die-mailkonten-der-bundeskanzlerin-knackten-a-00000000-0002-0001-0000-000170816296 (accessed 2 June 2021).

137 "Kurzprotokoll der 7. Sitzung" (see note 134).

138 Ibid. ["an etwa neun bekannte, weltweit verteilte, verdächtige Server"].

139 Ibid.

140 Anna Biselli, "Wir veröffentlichen Dokumente zum Bundestagshack: Wie man die Abgeordneten im Unklaren ließ", *Netzpolitik.org*, 7 March 2016, https://netzpolitik.org/2016/wir-veroeffentlichen-dokumente-zum-bundestagshack-wie-man-die-abgeordneten-im-unklaren-liess/ (accessed 21 May 2021).

website dcleaks.com was registered.[141] The idea that the attack aimed "to sow the seeds of discord or fuel anxieties" was a plausible explanation at the time, although the stolen material was never published, as is usual in classic espionage operations.[142] The political context of the U.S. election in 2016, however, is central to the subsequent legal and political assessment of an attack.

Attribution of the attackers

Although it is possible to glean information about the technical characteristics of the attack from public sources, the federal government kept these details, which were relevant to attribution, confidential. The BKA and German law enforcement officers also relied on public information gathered by U.S. authorities in the course of their investigation into the DNC hack.[143] The IT security firm ThreatConnect posted a blog entry describing how it managed to determine that the same certificate had been used in the attack on the U.S. Democrats in the 2016 election campaign and in the 2015 Bundestag hack.[144]

The development of the malicious program required substantial funding and support from an established organisation and probably a state.

Early on, in June 2015, Claudio Guarnieri speculated that the Russian-based group APT 28 was a possible originator. He based this on a report by IT security firm FireEye (2014), which claimed that APT 28 was funded by the Russian state. FireEye reached this conclusion on the basis of past operations that identified similar malware artefacts and TTPs. The attack tools were compiled on systems with Russian language settings during the usual Moscow and St. Petersburg office hours. The years of development behind the malware would have required substantial funding as well as support from an established organisation and "most likely" a state. The cyber operation's goals were consistent with Russia's foreign policy interests and strategies.[145] Guarnieri's arguments for attribution to APT 28 were corroborated by documentation from business consulting firm PricewaterhouseCoopers (PwC). According to the PwC report, certain IPs and SSL certificates that played a role in the Bundestag hack had previously been used in an attack that was attributed to the Sofacy/APT 28 group.[146]

In June 2015, the President of the Federal Office for the Protection of the Constitution, Hans-Georg Maaßen, suggested that a foreign intelligence service was responsible for the attack. He did not provide technical details.[147] A year later, Maaßen claimed that the Russian state was behind the attack.[148] Evidence was based on technical analysis, but also came from intelligence sources.[149]

In early 2018, the Dutch domestic and foreign intelligence service the AIVD (Algemene Inlichtingen en Veiligheidsdienst) publicised information about the hacker group APT 29, also known as Cozy Bear.[150]

141 "Diese 4 Webseiten deuten auf ein Bundestagsleak hin und hier steht warum" *Buzzfeed*, 8 August 2017, https://www.buzzfeed.de/recherchen/diese-webseiten-deuten-auf-ein-bundestagsleak-hin-und-hier-steht-warum-90134843.html (accessed 21 May 2021).

142 Diehl, Rosenbach and Schmid, "Rekonstruktion eines Cyberangriffs" (see note 136). ["Zwietracht säen oder Unsicherheit schüren"].

143 Florian Flade and Hakan Tanriverdi, "Der Mann in Merkels Rechner — Jagd auf Putins Hacker" (BR Podcast), Episode 4: Der Mann in Merkels Rechner, *BR Bayern 2*, 22 April 2021, https://www.br.de/mediathek/podcast/der-mann-in-merkels-rechner-jagd-auf-putins-hacker/853 (accessed 21 May 2021).

144 "Finding Nemo(hosts)", *Threatconnect Research*, 21 July 2017, https://threatconnect.com/blog/finding-nemohost-fancy-bear-infrastructure/ (accessed 2 June 2021). Timo Steffens provides a detailed account of this in his book: *Auf der Spur der Hacker. Wie man die Täter hinter der Computer-Spionage entlarvt*. (Berlin: Springer Verlag, 2018), 66ff.

145 FireEye, *APT28: A Window into Russian Espionage Operations?* (Milpitas, CA, 2014), https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-apt28.pdf (accessed 2 June 2021).

146 Guarnieri, "Digital Attack on German Parliament" (see note 135).

147 Patrick Beuth, "Hackerangriff im Bundestag: 'Das ist kein allzu großer Fall'", *Zeit Online*, 12 June 2015, https://www.zeit.de/digital/datenschutz/2015-06/bundestag-hack-karlsruher-firma-aufklaerung (accessed 2 June 2021).

148 "Russia 'was behind German parliament hack'", *BBC News* (online), 13 May 2016, https://www.bbc.com/news/technology-36284447 (accessed 2 June 2021).

149 "Hacker im Staatsauftrag — Netzwerk Recherche #nr17", *YouTube*, 9 June 2021, min. 6:50, https://www.youtube.com/watch?v=OfRb6hssfu8 (accessed 9 June 2021).

150 Huib Modderkolk, "Dutch Agencies Provide Crucial Intel about Russia's Interference in US Elections", *De Volkskrant*, 25 January 2018, https://www.volkskrant.nl/

According to media reports, the Dutch had hacked into the APT group's networks in 2014, gained access to surveillance cameras in the building where the hackers had their offices, and identified members of the APT as intelligence operatives. This finding was in turn corroborated by the investigation conducted by U.S. Special Investigator Robert Mueller. His April 2019 report and an earlier July 2018 indictment named 12 intelligence officers from units 26165 and 74455 of Russia's GRU military intelligence service as the perpetrators. The Mueller report supports the thesis that the GRU attackers used similar TTPs in different operations such as NotPetya, the OPCW hack and the Bundestag hack.[151]

After 2018, further states publicly declared the Russian government responsible for several cyber operations. In autumn 2018, the German government endorsed this view: "The German government also assumes with a probability bordering on certainty that the Russian military intelligence service GRU is behind the APT 28 campaign [...] This assessment is based on the government's own solid facts and reliable sources".[152] In November 2019, the Attorney General announced that the group APT28/Fancy Bear was being investigated.[153] After these investigations were concluded, in May 2020, Chancellor Merkel announced that there was "'hard evidence' for Russian involvement" and that this was an "outrageous" event.[154]

EU response to the Bundestag hack

On 22 October 2020, the Council of the European Union adopted sanctions against the 85th Main Special Services Centre (GTsSS) of the Main Directorate of the General Staff of the Armed Forces of the Russian Federation (GU/GRU) and its military intelligence officers Dmitry Badin and Igor Kostyukov by implementing Regulation (EU) 2020/1536.[155] The targeted sanctions were economic sanctions under Article 3 of Regulation (EU) 2019/796 and entry restrictions under Article 4 Decision (CFSP) 2019/797.[156] The grounds state that Dmitry Badin was involved as an agent of the GTsST in a cyberattack which had significant repercussions for the German Bundestag in April and May 2015. Igor Kostyukov, as head of the main directorate of the "military unit 26165" — known by experts as "APT28", "Fancy Bear", "Sofacy Group", "Pawn Storm" and "Strontium" — had carried out the hack. Both GRU operatives were declared responsible not only for the attack against the German Bundestag, but also for the attempted cyberattack in April 2018 on the Organisation for the Prohibition of Chemical Weapons (OPCW).[157]

wetenschap/dutch-agencies-provide-crucial-intel-about-russia-s-interference-in-us-elections~b4f8111b/ (accessed 2 June 2021).

151 U.S. Department of Justice, *Report on the Investigation into Russian Interference in the 2016 Presidential Election*, vol. I (Washington, D.C., March 2019), 36ff., https://www.justice.gov/archives/sco/file/1373816/download (accessed 21 May 2021); U.S. District Court for the District of Columbia, *United States of America v. Viktor Borisovich Netyksho, Boris Alekseyevich Antonov, Dmitriy Sergeyevich Badin and Others*, Indictment, CR 18-215, 13 July 2018, https://www.justice.gov/file/1080281/download (accessed 9 January 2021).

152 "Auch Bundesregierung macht Russland verantwortlich für Cyberangriffe", *Der Spiegel* (online), 5 October 2018, https://www.spiegel.de/netzwelt/netzpolitik/apt28-bundesregierung-beschuldigt-offiziell-russland-der-cyberangriffe-a-1231744.html (accessed 6 October 2021) ["Auch die Bundesregierung geht mit an Sicherheit grenzender Wahrscheinlichkeit davon aus, dass hinter der Kampagne APT 28 der russische Militärgeheim-dienst GRU steckt […] Diese Einschätzung beruht auf einer insgesamt sehr guten eigenen Fakten- und Quellenlage"].

153 Jörg Diehl and Fidelius Schmid, "Deutschland ermittelt gegen russische Hacker", *Der Spiegel*, 16 November 2019.

154 "Hackerangriff auf Bundestag: Angela Merkel erhebt schwere Vorwürfe gegen Moskau", *Der Spiegel* (online), 13 May 2020, http://www.spiegel.de/politik/deutschland/hackerangriff-angela-merkel-erhebt-schwere-vorwuerfe-gegen-moskau-a-36fc72c7-7f66-47e6-997d-fbd5a08ae4d5 (accessed 9 January 2021) ["von 'harten Evidenzen' für eine russische Beteiligung und von einem 'ungeheuerlichen' Vorgang"].

155 Council of the European Union, "Council Implementing Regulation (EU) 2020/1536 of 22 October 2020 Implementing Regulation (EU) 2019/796 concerning Restrictive Measures against Cyber Attacks Threatening the Union or its Member States", *Official Journal of the European Union*, no. L 351 I/1 (22 October 2020), https:// eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32020R1536 (accessed 2 June 2021).

156 Ibid., Annex.

157 Council of the European Union, "Council Implementing Regulation (EU) 2020/1125" (see note 107).

Attempted attack on the OPCW 2018

On 13 April 2018, four Russian intelligence agents prepared what is known as a WiFi spoofing attack[158] on the Organisation for the Prohibition of Chemical Weapons (OPCW) in The Hague. They parked a rental car in the car park of the Marriott Hotel next to the OPCW building that was rigged with a fake WiFi hotspot (known as a WiFi Pineapple). The manipulated Pineapple router was intended to imitate the OPCW's original WLAN. Such a procedure is called a man-in-the-middle attack.[159] WiFi spoofing only works if the fake WLAN is placed in direct physical proximity to the original. To do this, the perpetrators must be directly on site ("close access operation"). While conducting the operation, the attackers had been observed and were subsequently arrested by the Dutch Military Intelligence Service (Militaire Inlichtingen- en Veiligheidsdienst, MIVD). According to the *Guardian* newspaper, the Dutch had received a timely tip-off from British intelligence services.[160] The four GRU operatives had entered the country through Amsterdam's Schiphol Airport on 10 April 2018, and had been under surveillance since then.[161] Dutch security authorities intervened early to prevent a successful compromise of the OPCW. They seized diplomatic visas, a large sum of cash, technical equipment, smartphones, laptops, passports and travel receipts.[162] The attack was thus unsuccessful and inconsequential.[163]

Attribution of the attackers

Due to the timely arrest of the attackers, the attribution in this case turned out to be quite straightforward. The forensic analysis of the seized equipment allowed conclusions to be drawn not only about the target of the operation, but even about past and planned operations. Investigators acquired information on the poison attack on former GRU agent Sergei Skripal in Salisbury (UK). The nerve agent attack had taken place a month earlier, and the OPCW was tasked with its analysis. Travel logs showed that the next target on the perpetrators' list had been an OPCW lab in Switzerland. The equipment's WiFi logs also revealed that the group had previously travelled to Malaysia and Brazil. Temporal and spatial similarities with the results of the Dutch investigation into the shooting down of Malaysia Airlines flight MH17 and the 2016 Olympic Games in Brazil became evident.[164]

The call logs of the seized cell phones led directly to the GRU headquarters.

Following investigations by the World Anti-Doping Agency (WADA), Russian track and field athletes had been banned from the Olympic Games in Rio de Janeiro in July 2016 due to doping allegations. In September 2016, WADA had also been the victim of a cyberattack by the same team of hackers. The call logs of the seized mobile phones led directly to the GRU headquarters. Visas and taxi receipts, which a state intelligence agency needs to have costs for business trips reimbursed, confirmed the involvement of GRU unit 26165, which was also involved in the NotPetya attack and the Bundestag hack.

The political attribution was made by the Dutch government on 4 October 2018, in a lengthy press conference in which all the details of the investigation were shared. The Dutch stated that any incident

158 WiFi spoofing is based on users mistakenly logging into a hotspot with their regular user data.

159 Andy Greenberg, "How Russian Spies Infiltrated Hotel Wi-Fi to Hack Their Victims up Close", *Wired* (online), 4 October 2018, https://www.wired.com/story/russian-spies-indictment-hotel-wi-fi-hacking/ (accessed 25 May 2021).

160 Luke Harding, "How Russian spies bungled cyber-attack on weapons watchdog", *The Guardian* (online), 4 October 2018, https://www.theguardian.com/world/2018/oct/04/how-russian-spies-bungled-cyber-attack-on-weapons-watchdog (accessed 25 May 2021).

161 U.S. Department of Justice, *US v. Aleksei Sergeyevich Morenets* (Washington, D.C., October 2018), https://www.justice.gov/usao-wdpa/vw/us-v-Aleksei-Sergeyevich-Morenets (accessed 2 June 2021).

162 Onno Eichelsheim, "GRU close access cyber operation against OPCW", *Netherlands Ministry of Defence* (The Hague, 4 October 2018), https://english.defensie.nl/binaries/defence/documents/publications/2018/10/04/gru-close-access-cyber-operation-against-opcw/ppt+pressconference+ENGLISH+DEF.pdf.

163 U.S. Department of Justice, *US v. Aleksei Sergeyevich Morenets* (see note 161).

164 Government of the Netherlands, "Netherlands Defence Intelligence and Security Service Disrupts Russian Cyber Operation Targeting OPCW" (The Hague, 25 May 2021), https://www.government.nl/latest/news/2018/10/04/netherlands-defence-intelligence-and-security-service-disrupts-russian-cyber-operation-targeting-opcw (accessed 25 May 2021).

that undermined the integrity of international organisations was "unacceptable". The government in The Hague summoned the Russian ambassador, and the Dutch defence minister and the British ambassador condemned the GRU and, indirectly, the Russian government, for these attacks.[165] In the United States, on the same day of the press conference, charges were brought against seven Russian intelligence officers. They were said to be employees of GRU unit 26165,[166] who, in addition to attacking the OPCW, had also carried out attacks against the anti-doping agencies USADA, WADA and the Canadian Centre for Ethics in Sport (CCED).[167] Two months earlier, in August 2018, the U.S. had asked the Netherlands for legal assistance in prosecuting Russian cyber operations against U.S. and international organisations. The allegations and circumstantial evidence gathered in the CR 18-263 indictment on the case of the attempted OPCW attack are[168] consistent with the indications provided by the Dutch Ministry of Defence. The log data from the WiFi attack equipment showed that the attackers were in the same hotel at the same time when the laptop of a representative of the Canadian anti-doping agency CCED was infiltrated.

The absence of a legal attribution is remarkable. The Dutch waived charges and detained the convicted spies only for a short time. The day after their arrest, they were put on a plane to Russia and expelled from the country. The GRU operatives had official diplomatic passports, which protected them from prosecution. An officer of the Dutch intelligence service explained the situation as follows: "Hacking is a criminal offence. Attempting to hack is also a criminal offence. Preparing for an attempt to hack is not a criminal offence".[169] The OPCW hack is unique because it was not a classic cyberattack. The attack was stopped in time and was promptly publicised by the Dutch government, providing the EU with information for attribution of a level of detail that had not been available in any of the other incidents discussed so far. The transparency on technical, legal and political attribution is exemplary and leaves little room for erroneous conclusions.

EU response to the attempted attack on the OPCW

The Presidents of the European Council and the European Commission and the High Representative for Foreign Affairs and Security Policy first commented on the attempted cyberattack on the Organisation for the Prohibition of Chemical Weapons in a joint statement on 4 October 2018. They described the incident as "an aggressive act [that] demonstrated contempt for the solemn purpose of the Organisation for the Prohibition of Chemical Weapons (OPCW)…".[170] In this case, the timing of the political attribution worked: it was at least stringent and in concert with allies, and the signalling was clear. The EU sanctions were issued at the end of July 2020, with Implementing Regulation 2020/1125[171] and its addendum 2020/1744[172] from the end of November 2020. The restrictive measures are directed against the 85th Main Special Services Centre (GTsSS) within the GRU and its employees Alexey Minin, Aleksei Morenets, Evgenii Serebriakov and Oleg Sotnikov.[173]

165 Ibid.

166 U.S. Department of Justice, *US v. Aleksei Sergeyevich Morenets* (see note 161).

167 Ibid.

168 Ibid.

169 Flade and Tanriverdi, "Der Mann in Merkels Rechner — Jagd auf Putins Hacker" (BR Podcast) (see note 143), Episode 3: "Ganz nah dran", https://www.br.de/mediathek/podcast/der-mann-in-merkels-rechner-jagd-auf-putins-hacker/3-ganz-nah-dran/1823410 (accessed 21 May 2021).

170 European Council, "Joint Statement by Presidents Tusk and Juncker and High Representative Mogherini on Russian Cyber Attacks", press release, Brussels, 4 October 2018, https://www.consilium.europa.eu/de/press/press-releases/2018/10/04/joint-statement-by-presidents-tusk-and-juncker-and-high-representative-mogherini/ (accessed 30 September 2021).

171 Council of the European Union, "Council Implementing Regulation (EU) 2020/1125" (see note 107).

172 Council of the European Union, "Council Implementing Regulation (EU) 2020/1744" (see note 129).

173 Council of the European Union, "Council Implementing Regulation (EU) 2020/1125" (see note 107), Annex.

Shortcomings of the Attribution Policy

The analysis shows that the EU's attribution competence is deficient. It reveals the weaknesses of the current system of technical, political and legal identification of perpetrators. It shows the significant hurdles that still need to be overcome on the long road to an effective and legitimate "politics of attribution" at both the EU and intergovernmental levels.

First, the EU relies heavily on evidence and expertise from allied third countries, such as the Five Eyes alliance as well as U.S. IT companies. Evidence provided by the security services of EU Member States is usually deficient and incomplete. The OPCW attack would not have been uncovered and prevented in time without the tip-off from the UK authorities. The German investigation into the Bundestag hack was based on publicly available indictments and non-public exchanges with the FBI. Whether the exchange of information with the Five Eyes member Great Britain, which is necessary for attribution, will be maintained after Brexit remains to be seen.

Second, it is evident that in almost all the cases described, the EU responded with a time lag. The coordination processes and the unanimity required for cyber sanctions under the CFSP necessitate a lengthy attribution process, which in some cases took years longer than the convictions by the Five Eyes partners. This may be due to the complex technical forensics typical of cyber incidents, but is certainly partly also down to the parallel information sharing procedures at EU and Member State level. The responsibilities for cybercrime, cyber espionage and counter-intelligence, and military cyber defence lie primarily with the Member States and must be coordinated at EU level through Europol, in the EEAS through EU INTCEN, and in future also through the Joint Cyber Unit in the EU Commission.

With Brexit, the EU's power of attribution has diminished considerably.

Third, it is evident that the members of the Five Eyes alliance manage public attribution better than their EU counterparts: They coordinate with speed and efficiency and issue simultaneous pronouncements based on extensive evidence. Thus, the legitimacy of attribution is more solid than the EU's. With Brexit, the EU's attribution authority has diminished significantly, as the UK no longer shares intelligence through EU INTCEN, but still exchanges information bilaterally with selected EU states. Compared to Five Eyes, political attribution in support of EU cyber sanctions occurs infrequently and sporadically. A credible policy of attribution would require all Member States to speak with one voice. Political attribution remains the prerogative of the Member States. However, the impact of national attribution is limited. Pooling attribution reports at the EU level can significantly increase the legitimacy and effectiveness of a sanction decision. This is particularly true if the attribution of responsibility takes place in coordination with international partners. The so-called "naming and shaming" campaign by allies can only succeed if the respective foreign ministries act in a coordinated manner.

Fourthly, cyber sanctions are to be imposed in the event of attacks with a "significant impact" or if the relevant criteria are fulfilled. However, the analysis shows that it is difficult to determine from technical indicators and IoCs whether a criterion is actually fulfilled, which is required to legitimise a legal consequence such as sanctions. The known criteria of the cyber incidents analysed are rather ambiguous, do not take technical details into account to an adequate extent, and their weighting is also unclear. For example, the question arises as to whether an attack against an electoral system is more serious than an attack against critical infrastructure. Does an attack against

numerous less critical systems weigh more heavily than an attack against a hospital?[174] The problem of proving malicious intent emanating from third countries is illustrated by the following criteria:

a) The fulfilment of the criterion "*malicious* use of ICT" cannot be clearly determined in all cases. In the case of WannaCry and NotPetya, a sufficient degree of malice can indeed be established: due to the arbitrary selection of targets, the indifference to the disruption of critical infrastructures such as hospitals and the billions of euros in damage caused to states and companies. In other cases, malice is difficult to prove beyond reasonable doubt.

b) From a technical point of view, the criteria that are supposed to *define a cyberattack* (access to and interference with information systems and interference with data or the interception of data) cannot be clearly separated from each other. An intrusion in information systems is always synonymous with an intrusion into data, since defence systems are bypassed and malware is introduced, i.e. data is almost inevitably written on a file system. The same can be seen in the differentiation between *attacks* and *attempted attacks*: organisations with good detection systems receive thousands of security alerts every day. These are often not identifiable *a priori* as an attack, since the effect of an attack can only be recognised after malicious code has been executed. Only when the analysis of such code, combined with threat intelligence techniques, has identified information about attack infrastructures or tools of known APT groups, can affected organisations interpret the incident as a threatening act.

The strategic operational objective is difficult to derive from what are mostly purely tactical IoCs.

c) It is also difficult to derive the strategic *operational goal or motivation for the attack* from what are mostly purely tactical IoCs. In the case of WannaCry, for example, the motivation for the attack is not clear. The interpretation of the Bundestag hack as an attempt at election interference is also difficult to infer from the IoCs alone. The conclusion of "election interference" is based on contextual factors, i.e. the hybrid threat, which only became prevalent in transatlantic discourse years later, after the DNC hack in 2016.

d) There are inconsistencies in the *selection of cases that* prompted the EU to impose cyber sanctions. There was no plausible explanation for why, for example, cases of classical espionage (Bundestag hack and Cloud Hopper) were included in the cyber sanctions regime, but concrete attempts to influence elections (Macron leaks) were not. Espionage has been part of state practice for decades. While it is punishable under virtually all national legal systems, it is not illegal under international law.[175] During the hack of Emmanuel Macron's campaign team's emails in 2017, communications content was stolen and also leaked, analogous to the DNC hack, two days before runoff election day.[176] Unlike the Bundestag hack, this is a clear attempt to influence the electoral process, which goes beyond political espionage and can be considered a violation of state sovereignty. If the aim was to send a strong political signal, this incident should have been included in the 2020 cyber sanctions regime. The U.S. law enforcement agencies had, in the context of the NotPetya indictment, attributed responsibility for the Macron leaks to the Russian GRU.[177]

Office hours and IP addresses in the context of a cyberattack are merely than circumstantial evidence of an actor's authorship.

e) Moreover, it is questionable to what extent *technical attribution* allows for *plausible proof of legal responsibil-*

174 Julia Grauvogel and Christian von Soest, *Cybersanktionen: Zunehmende Anwendung eines neuen Instruments*, GIGA Focus — Global, no. 3 (Hamburg: German Institute of Global and Area Studies [GIGA], April 2021), https://pure.giga-hamburg.de/ws/files/24469713/gf_web_global_2021_03_D.pdf (accessed 14 September 2021).

175 If the leaked information had been instrumentalised in the 2017 German federal election campaign, as the internal emails of the Democratic National Committee in the U.S. had been in 2016, the legal concept of "illegal intervention" or "self-determination" could have applied.

176 Jean-Baptiste Jeangène Vilmer, *The "Macron Leaks" Operation: A Post-Mortem* (Washington, D.C.: *Atlantic Council*, June 2019), https://www.atlanticcouncil.org/wp-content/uploads/2019/06/The_Macron_Leaks_Operation-A_Post-Mortem.pdf (accessed March 1, 2021).

177 United States District Court Western District of Pennsylvania, *United States of America v. Yuri Sergeyevich Andrienko* (see note 106).

ity. From the analysis of cyberattacks in the EU so far, it is not always clear which technical IoCs constitute an adequate basis for a legal normative attribution of cyberattacks according to European law (or even international law). Office hours and IP addresses in the context of a cyberattack are merely circumstantial evidence, and not proof of authorship by an individual acting on behalf of the state. Taxi receipts, cell phone logs and hacked surveillance cameras at the GRU headquarters, on the other hand, have greater probative value. The discrepancy between the technical indicators and the legally required elements of the crime is evident: in the Bundestag hack and Cloud Hopper cases, the information published by the EU or the German government is sparse compared to the publicly available findings of IT security companies, the technical details in U.S indictments in similar cases, and the Dutch government's transparency campaign after the OPCW incident.

f) The inconsistency of the evidence and *lack of transparency of the* legal evidence impair the legitimacy of the sanctions. Making the scope of forensic evidence as broad as possible and comprehensible to the public would help make the sanctions more credible and effective. The U.S. indictments in the cases discussed here manages this to a far greater extent than the EU does with the justifications it publishes in the Official Journal. The U.S. also presents the evidence more assertively. The Member States should advocate a technically adept and legally sound legitimisation of cyber sanctions, in their own clearly understood self-interest, because EU sanction decisions can be legally challenged before the European Court of Justice.[178]

g) Another inconsistency can be seen in the standards of evidence, especially in the case of the Bundestag hack. According to the German federal government, the attribution made in this regard is based on what is generally a "very good situation when it comes to our own facts and sources".[179] In the other cases, the European, U.S. and British security authorities sometimes make an attribution "with near certainty", sometimes only with "a high degree of certainty". A Europe-wide, or better still transatlantic, standardised terminology and methodology would already be helpful in the case of mutual legal assistance requests. If, on top of that, information on the evidence were to be more systematically processed, categorised and published in close consultation with allied states in the future, cyber sanctions could be made much more plausible at the EU level than they have been so far.

Lastly, the *quality of the counterreactions*, i.e. the sanctions themselves, is also worthy of discussion. In all cases, travel restrictions were imposed and accounts frozen. For the Cloud Hopper cyberattacks, the Bundestag hack and the OPCW incident, this may be adequate and proportional. WannaCry and NotPetya, on the other hand, are much more serious cases. They meet far more and, above all, far weightier criteria for criminal offences, including major financial damage and sabotage of critical infrastructure. According to the legal opinion of some observers, NotPetya even reaches the threshold of an armed attack.[180] The intensity of the sanctions here does not appear to be proportionate to the intensity of the attacks. It could certainly be argued that in both cases there were clear violations of sovereignty that would have permitted countermeasures under international law.[181] Rapid and differentiated EU sanctions in response to cyberattacks will remain the exception for the foreseeable future. The coherence of the sanctions process should be improved by means of a reformed Commission Blueprint (see above, p. 14). Alongside Europol, ENISA and the EU-CERT, the Commission's newly created Joint Cyber Unit will play an important role in European cybersecurity in the future. However, in future, the EU Commission will certainly not be in a position to steer the attribution policy pursued by the EU on its own. On this issue in particular, the Commission will be dependent on close consultation with the Council and the Council's Horizontal Working Party on Cyber Issues.

178 Ivan, *Responding to Cyberattacks* (see note 102).

179 "Cyberattacken: Regierung beschuldigt Russland offiziell", *Süddeutsche Zeitung* (online), 5 October 2018, https://www.sueddeutsche.de/service/internet-cyberattacken-regierung-beschuldigt-russland-offiziell-dpa.urn-newsml-dpa-com-20090101-181005-99-250924 (accessed 2 June 2021).

180 Piret Pernik, "Responding to 'the Most Destructive and Costly Cyberattack in History'" (Tallinn: International Centre for Defence and Security [ICDS], 23 February 2018), https://icds.ee/en/responding-to-the-most-destructive-and-costly-cyberattack-in-history/ (accessed 2 June 2021).

181 Alex Hern, "'NotPetya' Malware Attacks Could Warrant Retaliation, Says NATO Affiliated-researcher", *The Guardian* (online), 3 July 2017, https://www.theguardian.com/technology/2017/jul/03/notpetya-malware-attacks-ukraine-warrant-retaliation-nato-researcher-tomas-minarik (accessed 2 June 2021).

Conclusions

The EU's attribution policy shows that vertical, horizontal and institutional coherence in the EU's external action and between EU Member States leaves much to be desired. The requirement for unanimity in the Council's decision-making and the lack of legal and financial resources for the EEAS make it difficult for the EU to make its mark in international cyber diplomacy. The German government should support the French Council Presidency in making qualified majority voting the norm for the adoption of EU cyber sanctions. In the interest of the security of the Union and its internal market, restrictive CFSP measures, such as EU cyber sanctions, should be initiated and reliably imposed more quickly than in the past in order to promptly bring perpetrators and attackers to justice.

The legal terms in the EU regulations should be tightened and more closely related to technical forensics. A number of prerequisites must be met in the practical implementation of this task. After all, for an unambiguous technical attribution that allows conclusions to be drawn about the motivation for the attack, high legal hurdles have to be overcome if the criteria set out in the relevant regulation are to be met, something which is essential for determining authorship. Ideally, the attribution policy would need to be adapted to the legal requirements. If this does not prove possible, if necessary, the law would have to be adapted. The introduction of a distinction between necessary and sufficient attribution standards in accordance with a uniform evaluation system (probability yardstick) would at least have to be reconciled with the constitutional requirements of Union law and the current possibilities of technical forensics. Experience from other international cyberattacks can also be drawn upon. For example, there were comparable supply chain attacks before Operation Cloud Hopper. The latter proved to malicious hackers just how attractive such an attack on the domestic market was. The response to supply chain attacks should therefore be practised by means of ENISA cyber defence exercises, in line with the Commission's recommendations in the Blueprint document.

According to the new EU Cybersecurity Strategy of 2020, private companies, public institutions and national authorities should systematically and comprehensively share information on cyber incidents. This is seen as a prerequisite for a joint EU response. The EU Commission's Joint Cyber Unit is to serve as a "virtual and physical platform of cooperation between the different cybersecurity communities in the EU". Its focus is to be on "operational and technical coordination on serious cross-border cyber incidents and threats". This operational cooperation in the service of cybersecurity is to be heightened in line with the due diligence responsibilities of cyber diplomacy. The Cyber Unit is also intended to be a hub for communication with the Five Eyes alliance to enable joint public attributions beyond EU borders.

There is also now a debate about the extent to which EU governments and the EU should equip themselves to carry out counter-attacks. The Cybersecurity Strategy already contains a reference to this and cases like WannaCry and NotPetya underline the urgency. Accordingly, the EU wants to develop a "proposal to further define EU cyber deterrence". According to the cyber diplomacy toolbox, active cyber defence measures would be the highest escalation level after prior activation of the treaty-based solidarity or mutual assistance clause. They can only be taken provided that they are in accordance with international humanitarian law. The final stage of crisis management would be to stop an ongoing attack by actively countering it. The last resort would be what is known as a "hack back", i.e. the targeted disabling of a server from which an attack originates. In terms of due diligence, this would only be justifiable if an ongoing attack has severe, existence-threatening consequences and all other means have been exhausted. The necessary legal framework and distribution of competences have not yet even been established at national level, not to mention the EU-level legal arrangements for the attribution procedure required for this. As things stand at present, crisis management in which all 27 Member States would have to agree to activate a digi-

tal cyber defence is likely to prove too complex and too slow in an emergency.

This makes it all the more important to strengthen the EU's attribution competence and IT security in the internal market. Notwithstanding the undoubtedly correct understanding that many preconditions must be met for reliable attribution, it is a requirement for the enforcement of the rule of law that perpetrators and attackers are held accountable. Therefore, developing analytical capabilities is a necessary condition worth investing in. Similarly, mandatory IT baseline protection must be maintained in the EU. New legislation, such as the reform of the current Network and Information Security Directive, and the Cyber Resilience Bill announced by Internal Market Commissioner Thierry Breton in September 2021, are right to focus on securing infrastructure, cloud services and supply chains more broadly. However, the requirement for corporations to take precautions against cybersecurity threats is not currently resulting in the required level of investment in building resilient IT systems; instead funds are flowing into the purchase of cyber insurance policies. The cause and success of numerous attacks lie in the inadequate protection of basic software, which often is developed in the USA, where companies are not liable for the shortcomings of their programs. Consequently, if we want to avoid a situation where laws on each side of the Atlantic counteract each other, close transatlantic coordination is also needed at this point.

The most important and sustainably effective measures of operational cooperation within the Union and with the Five Eyes partners are prevention and detection. As shown by the discrepancy between the detection of technical IoCs and political or legal attribution, the political assessment of an incident in the context of a strategic situation analysis by the Hybrid Fusion Cell in the EEAS plays a particularly important role. It must take into account the bigger picture of incidents in cyberspace, because hybrid threats of military relevance can also be expected. To this end, it would make sense to collect data on past and current attack campaigns, suspected perpetrators, targets, the number of Member States affected, damage incurred and its legal classification in a kind of cyber conflict database and to make this information available to the Member States. This is more likely to lead to a common understanding of the incidents and ideally to a coherent response. To achieve this, the EEAS would need more technically skilled and legally qualified scientific staff. Only reliable forensics will allow for strategically substantive situational awareness.

While, with its technical competencies, the EU's existing CSIRT network helps facilitate an exchange of comparable data on the protection of critical infrastructure, the Joint Cyber Unit in the EU Commission must be expanded for improved EU attribution management. Cyber diplomacy requires continuous communication between national security authorities, industry and academia. This is the responsibility of the Joint Cyber Unit, which in turn can only fulfil it in close consultation with the EEAS within the Single Intelligence Analysis Capacity. Public and private CERT alliances and mergers in industry are also essential for pooling expert knowledge on cyber diplomacy. As mentioned above, consideration could be given to drawing a distinction between sufficient and necessary attribution standards. In order for cyber diplomacy issues to function more smoothly at the interfaces between the Council and the Commission in the future, together with EU INTCEN, the Commission's Joint Cyber Unit and Europol (EC3) could jointly manage these intersections. As an institution, Europol would be particularly well suited to soften the competence boundaries between the CFSP procedure of the EEAS and the Commission's crisis management procedure. Ultima ratio would be the creation of a dual role at the highest level in the capacity of the President of the European Council and the President of the Commission. In the event of a merger, the strategic situation assessment for the protection of the internal market and the EU Security Union would then be a supranational competence.

Appendix

Glossary

Advanced persistent threat (APT)
An advanced persistent threat is when a well-trained, typically state-controlled individual attacks a network or system in a very targeted manner over an extended period of time for the purposes of espionage or sabotage, possibly moving and/or spreading within that network or system and thus gathering information or manipulating it.
https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Gefaehrdungen/APT/apt.html

Backdoor
A backdoor is a program, usually installed by viruses, worms or Trojan horses, that gives third parties unauthorised access ("backdoor") to a computer, but remains hidden and bypasses the usual security devices. Backdoors are often used for denial-of-service attacks that target the availability of services, websites, individual systems or entire networks.
https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Glossar-der-Cyber-Sicherheit/Functions/glossar.html?nn=522504&cms_lv2=132796

Bootloader
A bootloader is a computer program that is loaded by the firmware of a computer after start-up. A bootloader is launched by a bootable medium and then executed. The bootloader then loads other parts of the operating system, usually the kernel.
https://en.wikipedia.org/wiki/Bootloader

Bug / Vulnerability / Security gap
Bugs refer to errors in programs. A vulnerability is a security-related error in an IT system or an institution. This can be caused by the design, the algorithms used, the implementation, the configuration, the operation or the organisation. A vulnerability can be exploited resulting in a threat resulting in damage to an institution or system. If a vulnerability exists, an object (an institution or a system) is susceptible to threats.
https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Glossar-der-Cyber-Sicherheit/Functions/glossar.html?nn=522504&cms_lv2=132814

Command & Control Server (C2)
After infecting a system, most malicious programs contact the attackers' control server (C&C server) on the Internet in order to reload further malicious code from there, to receive instructions or to transmit information (such as user names and passwords) uncovered on the infected system to this server. Contact is often made using domain names registered by the perpetrators specifically for this purpose.
https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Glossar-der-Cyber-Sicherheit/Functions/glossar.html?nn=522504&cms_lv2=132798

DNS
The Domain Name System (DNS) assigns the corresponding IP address to addresses and names used on the Internet, such as www.bsi.bund.de.
https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Glossar-der-Cyber-Sicherheit/Functions/glossar.html?nn=522504&cms_lv2=132772

Domain controller
The domain controller is a server that centrally manages and controls a domain and its various objects. Users who want to log on to a network domain first contact the domain controller responsible for their domain.
https://www.ip-insider.de/was-ist-ein-domaenencontroller-a-626094/

EternalBlue
Eternalblue is an exploit that takes advantage of programming flaws in the SMB implementation (also known as NetBIOS or Common Internet File System) of the Windows operating system. The vulnerability is known as CVE-2017-0144 (SMB Remote Windows Kernel Pool Corruption).
https://de.wikipedia.org/wiki/EternalBlue

Exploit
An exploit is a method or program code that can be used to execute unintended commands or functions via a vulnerability in hardware or software components. Depending on the type of vulnerability, an exploit can be used, for example, to crash a program, extend user rights or execute arbitrary program code.
https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Glossar-der-Cyber-Sicherheit/Functions/glossar.html?nn=522504&cms_lv2=132800

Five Eyes
Five Eyes is an intelligence alliance consisting of the U.S., UK, Canada, Australia and New Zealand.
https://en.wikipedia.org/wiki/Five_Eyes

Indicators of compromise
Indicators of compromise (IoCs) comprise technical information that can be used to detect malware infection or other compromise. These are often network-based signatures, such as the domain names of control servers or host-based signatures that are searched for on the terminal device (such as hash sums characterising malware, entries in the Windows registry or similar).
https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Glossar-der-Cyber-Sicherheit/Functions/glossar.html?nn=522504&cms_lv2=132764

Industroyer
Industroyer is a malware believed to have been used in the cyberattack on Ukraine's power grid on 17 December 2016. The attack cut off power to one-fifth of the capital, Kyiv, for an hour. It is the first known malware designed specifically to attack power grids.
https://malpedia.caad.fkie.fraunhofer.de/details/win.industroyer

IP
This is an address which makes a computer accessible within a network according to the Internet protocol. An IP address consists of four bytes separated by dots: for example, 194.95.179.205.
https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Glossar-der-Cyber-Sicherheit/Functions/glossar.html?nn=522504&cms_lv2=132764

Keylogger
A keylogger is a piece of hardware or software that is used to log a user's keystrokes on the keyboard of a computer and thus monitor or reconstruct them.
https://de.wikipedia.org/wiki/Keylogger

Mimikatz
Mimikatz is a free and open source program for Microsoft Windows that can be used to display cached credentials by exploiting vulnerabilities.
https://de.wikipedia.org/wiki/Mimikatz

MSP
A managed services provider (MSP) is an information technology service provider that assumes and manages responsibility for providing a defined set of services to its customers.
https://de.wikipedia.org/wiki/Managed_Services_Provider

Patch
A patch is a software package with which software manufacturers close security gaps in their programs or introduce other improvements. Many programs facilitate the installation of these updates through automatic update functions. Patch management refers to processes and procedures that help to obtain, manage and apply available patches for the IT environment as quickly as possible.
https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Glossar-der-Cyber-Sicherheit/Functions/glossar.html?nn=522504&cms_lv2=132810

Phishing
The term "phishing" is a combination of "password" and "fishing". Phishing is an attempt to obtain access data for a service or a website, for example, by means of fake emails and/or websites. If this manipulation is not recognised by the victim and the authenticity of a message or website is not questioned, the victim may

unwittingly give their access data to unauthorized persons.
https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Glossar-der-Cyber-Sicherheit/Functions/glossar.html?nn=522504&cms_lv2=132810

Ransomware
Ransomware refers to malware that restricts or prevents access to data and systems and only releases these resources again upon payment of a ransom. This is an attack on the security objective of availability and a form of digital extortion.
https://www.allianz-fuer-cybersicherheit.de/Webs/ACS/DE/Informationen-und-Empfehlungen/Informationen-und-weiterfuehrende-Angebote/Glossar-der-Cyber-Sicherheit/Functions/glossar.html?cms_lv2=132812

RAT (remote access Trojan)
A remote access Trojan (RAT) is a type of malware that allows the attacker complete remote control over a system. When a RAT enters a computer, it allows the hacker to easily access local files, secure login authorisation and other sensitive information, or it uses this connection to download viruses that could be inadvertently shared with others.
https://heimdalsecurity.com/blog/what-is-a-remote-access-trojan-rat/

Single point of failure
A single point of failure (SPOF) is a component of a technical system whose failure results in the failure of the entire system.
https://de.wikipedia.org/wiki/Single_Point_of_Failure

SMB
Server Message Block (SMB), originally called Common Internet File System (CIFS), is a network protocol for file, print and other server services in computer networks. It is a central part of the network services of the Windows product family and allows access to files and directories located on another computer.
https://de.wikipedia.org/wiki/Server_Message_Block

SSL certificate
An SSL certificate is a small data file that digitally binds a cryptographic key to an organisation's details. When installed on a web server, it activates the security lock and https protocol and enables secure connections from a web server to a browser. Typically SSL is used to secure credit card transactions, data transfers and logins. SSL is increasingly becoming the norm for securing social media site browsing. SSL certificates bind together a domain name and an organisational identity.
https://www.globalsign.com/de-de/ssl-information-center/was-ist-ein-ssl-zertifikat

TTP (Tools, tactics and procedures)
This is the overall picture of attack behaviour that results from the means used, the tactics and techniques employed, and the preferred procedures of an actor. A tactic is the high-level description of behaviour; techniques provide a more detailed description of behaviour in the context of a tactic; and procedures provide a lower-level, highly detailed description of behaviour in the context of a technique.
https://csrc.nist.gov/glossary/term/Tactics_Techniques_and_Procedures

Wiper
A wiper is a class of malware whose goal is to wipe the hard drive of the computer it infects.
https://en.wikipedia.org/wiki/Wiper_(malware)

Zero day
The exploitation of a vulnerability that is known only to the discoverer is called a zero-day exploit. The public, and in particular the manufacturer of the affected product, usually only become aware of the vulnerability when attacks are discovered that exploit it. The term zero day is therefore derived from the fact that a corresponding exploit already existed before the day on which the manufacturer became aware of the vulnerability — i.e. on a fictitious "day zero". Consequently, the manufacturer has no time to protect users from the first attacks.
https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Glossar-der-Cyber-Sicherheit/Functions/glossar.html?nn=522504&cms_lv2=132776

Abbreviations

AIVD	Algemene Inlichtingen- en Veiligheidsdienst (intelligence and security agency of the Netherlands)
APT	Advanced persistent threat
BBC	British Broadcasting Corporation
BKA	Federal Criminal Police Office
BSI	Federal Office for Information Security (Bonn)
C2	Command & Control (Server)
CCDCOE	NATO Cooperative Cyber Defence Centre of Excellence
CCED	Canadian Centre for Ethics in Sport (Ottawa)
CERT	Computer Emergency Response Team
CFSP	Common Foreign and Security Policy
CIA	Central Intelligence Agency (USA)
CIR	Cyber and Information Domain Service
Coreper	Permanent Representatives Committee
CRITIS	International Conference on Critical Information Infrastructures Security
CSIRT	Computer Security Incident Response Team
DNC	Democratic National Committee (USA)
DNS	Domain Name System
EC3	European Cybercrime Centre (at Europol)
ECJ	European Court of Justice
EEAS	European External Action Service
ENISA	European Union Agency for Cybersecurity
EU INTCEN	European Union Intelligence and Situation Centre
EU LE ERP	EU Law Enforcement Emergency Response Protocol
EUMS	European Union Military Staff
FBI	Federal Bureau of Investigation (USA)
GCHQ	Government Communications Headquarters (UK)
GIGA	German Institute of Global and Area Studies (Hamburg)
GRU	Glavnoye Rasvedyvatelnoye Upravleniye (Russian Military Intelligence)
GTsSS	Glavnii Centr Specialnoy Slushbi (85th Main Centre for Special Services of the Main Directorate of the General Staff of the Armed Forces of the Russian Federation)
GTsST	Glavnii Centr Specialnych Technologii (Main Centre for Special Technologies of the Main Directorate of the General Staff of the Armed Forces of the Russian Federation)
HR	High Representative (High Representative of the Union for Foreign Affairs and Security Policy)
HWPCI	Horizontal Working Party on Cyber Issues (also: HWP Cyber)
HWP ERCHT	Horizontal Working Party on Enhancing Resilience and Countering Hybrid Threats
ICDS	International Centre for Defence and Security (Tallinn)
ICJ	International Court of Justice
ICT	Information and communication technology
ILC	International Law Commission
INTCEN	see EU INTCEN
IoC	Indicator of compromise
IP	Internet protocol
IPCR	Integrated Political Crisis Response (EU)
IS	Islamic State
JCAT	Joint Cybercrime Action Taskforce (at Europol)
MIVD	Militaire Inlichtingen- en Veiligheidsdienst (military intelligence service of the Netherlands)
MSP	Managed service provider
NCSC	National Cyber Security Centre (UK)
NIS	Network and Information Security (Directive, EU)
NSA	National Security Agency (USA)
OPCW	Organisation for the Prohibition of Chemical Weapons
OSINT	Open Source Intelligence
PSC	Political and Security Committee
RAT	Remote access Trojan
SIAC	Single Intelligence Analysis Capacity
SMB	Server Message Block
SOCMINT	Social media intelligence
SPOF	Single point of failure
TEU	Treaty on European Union
TFEU	Treaty on the Functioning of the European Union
TTP	Tools, techniques and procedures
UN	United Nations
USADA	United States Anti-Doping Agency
VP	Vice-President of the EU Commission
VPN	Virtual private network
WADA	World Anti-Doping Agency (Montreal)

Comparison table of cases (online only)

Table can be accessed at
https://bit.ly/SWP21RP10Annex