October 2023 · Christina Rupp & Dr. Alexandra Paulus

Official Public Political Attribution of Cyber Operations

State of Play and Policy Options

Stiftung Neue Verantwortung

Think Tank at the Intersection of Technology and Society

Acknowledgment

This analysis has been supported by the cyber diplomacy working group 'Cyber Norms on Attribution' and experts through interviews, online collaboration, and virtual country-specific focus group workshops. The views and opinions expressed in this paper are those of the authors and do not necessarily reflect the official policy or position of the experts or that of their respective employer/s. In alphabetical order, acknowledging essential contributions of:

- Greg Austin, University of Technology Sydney
- Justin Bassi, Australian Strategic Policy Institute
- Rebecca Beigel, Stiftung Neue Verantwortung
- Isabella Brunner, University of Vienna
- Michael Daniel, Cyber Threat Alliance
- Kristen Eichensehr, University of Virginia School of Law
- Jason Healey, Columbia University SIPA
- Sven Herpig, Stiftung Neue Verantwortung
- Garrett Hinck, Columbia University
- Bart Hogeveen, Australian Strategic Policy Institute
- Henning Lahmann, Leiden University
- Eugenia Lostri, Lawfare Institute
- Dai Mochinaga, Shibaura Institute of Technology
- Saher Naumaan
- Takashi Seto, National Institute for Defense Studies Japan
- Wilhelm Vosse, International Christian University (ICU) Tokyo
- Moritz Weiss, LMU Munich
- Kerstin Zettl-Schabath, Heidelberg University

Additionally, the authors would like to thank Luisa Seeling and Alina Siebert for their support with this publication.

Gefördert durch:
DSF Deutsche Stiftung Friedensforschung
german foundation for peace research

SPONSORED BY THE
Federal Ministry of Education and Research

This project was funded by the German Foundation for Peace Research (DSF) in conjunction with a grant from the German Federal Ministry of Education and Research (BMBF).

Executive Summary

When states become the target of malicious cyber activity, they have various options for responding politically. Which option states pursue depends primarily on whether they know who is behind a cyber operation. It is therefore essential to identify the perpetrator(s) of a cyber operation, a process also known as attribution. While states can engage in different forms of attribution, official public political attribution—a government entity's public disclosure of information tying malicious cyber operations to another state through official channels—represents the most significant form from a cyber diplomacy standpoint.

In recent years, official public political attributions have gained traction as they allow states to highlight that they consider the attributed activity inappropriate, deter similar activities in the future, and raise awareness about threats. However, although more and more states are using official public political attributions, there is no clear shared understanding among states regarding how states should do so responsibly. In relation to international security, such common understandings can contribute to preventing misunderstandings and increasing the predictability of inter-state conduct.

To stimulate an international strategic debate on this policy instrument that may eventually lead to a shared understanding, this analysis provides an overview of the current state of play and the policy options at a state's disposal when engaging in official public political attributions of cyber operations. To do so, it focuses on the practices of four countries—Australia, Germany, Japan, and the U.S. Based on a comparison of 164 official public political attributions by the four selected states—109 by the U.S., 32 by Germany, 17 by Australia, and 6 by Japan—this paper proposes and applies an analytical framework of 13 parameters with corresponding options that serves to identify similarities and differences—areas of convergence and divergence—across countries.

Overview of Parameters

1. Choice of communication channel
2. Selection of government entity(ies) communicating the OPPA
3. Factual description of the operation attributed
4. Provision of details on the attributed actor
5. Inclusion of a message to the attributed actor
6. Provision of or reference to evidence
7. Inclusion of estimative probability
8. Engagement in international cooperation and coordination efforts
9. Specification of the severity of the operation attributed
10. Formulation of policy objectives pursued with OPPA
11. Linkage to national (attribution) policy
12. Inclusion of reference to prior OPPAs
13. Reference to cyber norms or other commitments

In examining these cases, this analysis has found the following:

1. **Communication channels and designated government entities vary across countries and over time.** The focus countries' practices varied in that states used and prioritized different types of channels, including political, technical, criminal law channels and economic sanctions channels, to communicate their official public political attributions. The focus countries were similar in that especially their Ministries of Foreign Affairs and national cybersecurity, intelligence, or law enforcement agencies acted as communicators of the official public political attribution.
2. **Official public political attributions always provide details on the operations attributed.** Many official public political attributions emphasized the targets or victims of the operations, followed by information on when the operations took place. At times, states also mentioned the damage and harm caused by the operations attributed.

3. **Official public political attributions differ in how they specify the attributed actor and sometimes include a message addressed to the actor.** The focus countries published attributions with varying levels of specificity, ranging from attributions mentioning individuals working for entities of a particular state to attributions with exclusive references to Advanced Persistent Threat groups, with a tendency toward increased specificity in recent years. States sometimes included appeals to the attributed actor to cease the operation attributed and expressed that they reserved the right to initiate further consequences.
4. **Only some official public political attributions mention evidentiary information and estimative probability.** The focus countries occasionally mentioned technical evidence and cited governmental and non-governmental sources in their attribution decisions, with a slight increase in the amount of mentions and citations over time. States sometimes provided specific technical information to support their political attributions. In a few instances, states included levels of confidence or likelihood to quantify the certainty of their attribution assessments.
5. **States increasingly coordinate their official public political attributions with like-minded countries.** The focus countries coordinated their official public political attributions internationally in three main ways: participating in internationally coordinated attributions, supporting public attributions of another state with or without their own attribution assessment, and retrospectively endorsing the official public political attribution of another state. In recent years, the focus countries predominantly used the first way through joint statements or advisories, either through ad hoc, like-minded constellations or institutionalized processes within the EU.
6. **States regularly explain why they attribute, pointing to the operation, their policies, and/or international commitments.** The focus countries often provided reasoning for why they attributed a particular cyber operation, especially when using political channels, by outlining the severity of the operation, formulating policy objectives, linking the attribution to general policy, referencing prior official public political attributions, or alluding to international commitments.

Given the varied ways in which states carried out their official public political attributions, the degree and scope of international convergence regarding how to conduct official public political attribution is limited among the four states at present.

For official public political attribution to mature as a policy instrument, a nuanced international policy debate is required, and decision-makers should seek ways to increase convergence, despite, or precisely because of, the topic's sensitivity. Since many states are currently either systematizing or establishing their policies and processes on (public) attribution, there is a political momentum for inter-state exchanges to build and operationalize shared understandings.

Table of Contents

1. Introduction

As society becomes increasingly digitized and cyber operations evolve in quality and quantity, the likelihood of public and private entities being compromised is growing. A measurable portion of such compromises is the product of the work of states or associated actors[1] who increasingly conduct cyber operations. Although remaining a complex task, finding out who the perpetrator of such operations was or is—a process referred to as attribution—is facilitated by maturing and improving methods for analyzing evidence and governmental attribution capabilities.[2]

When states know who is behind a cyber operation, they face the choice of whether they want to attribute political responsibility for these activities publicly—either stand-alone or in the context of other response instruments.[3] States may be interested in tying a malicious cyber operation to another state publicly, for example, to highlight that they consider the behavior inappropriate and establish accountability[4], to deter similar activities from reoccurring in the future, or to raise general awareness about cyber threats. At the same time, making an attribution public through official channels may also result in the revelation of intelligence information or draw repercussions from the government named politically responsible. In recent years, states have increasingly solved this trade-off in favor of publicly disclosing information tying cyber operations to another state through official channels. This analysis zooms in on these practices referred to throughout this study as official public political attribution (OPPA).

Such public attributions have been conducted by more and more states.[5] The U.S. Department of Justice (DOJ) did so for the first time in 2014, "charg[ing] five Chinese military hackers for cyber espionage against U.S. corporations and a labor organization for commercial advantage."[6] Additionally, states that find themselves frequently at the receiving end of other states' public attributions have also progressively begun

1 Jason Healey (2012): Beyond Attribution: Seeking National Responsibility for Cyber Attacks, Atlantic Council.
2 For a long time, attribution was deemed impossible—inter alia, due to possibilities of anonymization and concealment of usage behavior in the use of information and communications technologies (ICTs)—and labeled as the "attribution problem" (for example, Jon Lindsay (2015): Tipping the scales: the attribution problem and the feasibility of deterrence against cyberattack, in: Journal of Cybersecurity 1 (1), pp. 53-67) impeding a state's response options in countering cyber operations.
3 Sven Herpig (2021): Die Beantwortung von staatlich verantworteten Cyberoperationen, Stiftung Neue Verantwortung.
4 On the role that political attribution can play in creating accountability for UN cyber norms see also Jim Lewis (2022): Creating Accountability for Global Cyber Norms, Center for Strategic and International Studies.
5 As of August 8, 2023, the European Repository of Cyber Incidents (EuRepoC) lists 259 incidents matching the category "attribution by receiver government/state entity" when selected as "attribution basis" (EuRepoC (n.d.): Cyber Incidents).
6 DOJ (2014): U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage.

to publicize their respective claims.[7] For instance, in June 2023, the Russian Federal Security Service (FSB) deemed the U.S. National Security Agency (NSA) politically responsible for compromising "thousands of Apple phones to spy on Russian diplomats."[8]

Even though the number of attribution cases has increased and a growing number of states have made use of OPPA, there is no clear shared understanding among states on how to conduct OPPAs responsibly. For the purposes of this analysis, responsible OPPA reflects standards of appropriate behavior when publicly attributing a cyber operation to another state in accordance with the objective of maintaining international stability and security.[9] This can occur in the form of specifying positive duties or precluding certain actions. Shared standards on OPPA can contribute to international security by increasing the predictability of inter-state conduct—at least when states abide by them. In 2015, all United Nations (UN) Member States agreed on a catalog of 11 voluntary, non-binding cyber norms. However, given their abstract nature, these norms leave open and consequently give states ample room for interpretation as to how they should publicly communicate their attributions.[10] Since OPPAs offer states the opportunity to react to threats from other states and require intelligence information, they are often considered a matter of national security, which can complicate substantial international discussions on the matter.[11]

A few states have tried to put (public) attribution on the international agenda, inter alia, calling for "additional guidance on this important topic,"[12] the provision of "explanatory guidance on attribution,"[13] the "deepening [of] inter-state exchange and the sharing

7 In 2020, China also started to make use of public attributions and has since, for example, alleged that the U.S. National Security Agency would have compromised a Chinese military research university (Alexander Martin (12.09.2022): Beijing rebukes U.S. over alleged cyberattack on Chinese university, The Record).

8 Daryna Antoniuk (01.06.2023): Russia accuses US of hacking thousands of Apple devices to spy on diplomats, The Record.

9 This understanding of responsible OPPA builds upon Tim Maurer's definition of cyber norms (see further Tim Maurer (2019): A Dose of Realism: The Contestation and Politics of Cyber Norms, in: Hague Journal on the Rule of Law 12, pp. 283-305).

10 Norm (b) only mentions that "in case of ICT incidents, States should consider all relevant information, including the larger context of the event, the challenges of attribution in the ICT environment and the nature and extent of the consequences" (UN General Assembly (GA) (2015): Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (A/70/174)). The wide scope for implementing norm (b) has also not been thoroughly narrowed by the subsequent 2021 Group of Governmental Experts (GGE) report (UNGA (2021): Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security (A/76/135)). Whereas it, for example, refers to the need to "consider all aspects [...] such [as...] the incident's technical attributes; its scope, scale and impact; the wider context, including the incident's bearing on international peace and security; and the results of consultations between the States concerned", engaging in international coordination and exchanges, as well as noting the possibility of national policies and processes, it does not provide practical and detailed guidance on how these could be enforced in practice and what aspects states should consider and observe when publicly communicating their attribution findings.

11 For instance, the issue of attribution also featured among the areas of contention that stood in the way of the 2016-2017 UN GGE from reaching a consensus (for example, Michael Schmitt and Liis Vihul (2017): International Cyber Law Politicized: The UN GGE's Failure to Advance Cyber Norms, Just Security).

12 United States of America (2022): United States remarks for March 2022 session of the OEWG, as prepared.

13 Swiss Confederation (2023): Déclaration sur règles, normes, et principes de comportement responsable de l'État.

of best practices regarding the attribution of cyber incidents,"[14] or responded to the proposal to establish an "international attribution mechanism."[15] Yet, none of these attempts led to a comprehensive international discussion on how states can and should practice public political attribution in a responsible manner.[16] UN Member States merely agreed that "future work at the United Nations could also consider how to foster common understandings and exchanges of practice on attribution."[17]

Although there is yet to be a comprehensive international debate on public attribution, a number of developments suggest that the issue is becoming more relevant to states. First, attribution is playing an increasingly central role within a state's overall response toolkit to cyber operations as many policy instruments, such as sanctions, often build upon it.[18] Second, states have begun to institutionalize their domestic decision-making process in the form of national attribution processes or policies and have started to be more forthcoming about it.[19] Third, a growing number of states is seeking to acquire the necessary capabilities to engage in attribution in the first place.[20] All of these developments may lead to more OPPAs by more states in the future.

Against this backdrop, this analysis seeks to take stock of past national OPPA practices. Assuming that these practices at least implicitly reflect ideas about how to conduct OPPAs responsibly—that is, how states consider OPPAs should (not) be communicated—this stock-taking exercise permits to identify how states currently

14 Federal Republic of Germany (2022): German Statement at the July OEWG, Agenda Item 5, Section B.

15 For example, UNGA (2021): Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security. Chair's Summary (A/AC.290/2021/CRP.3); Japan (2021): Statement by Mr. Akahori Takeshi, Ambassador for United Nations Affairs and Cyber Policy of the Ministry of Foreign Affairs of Japan, at the United Nations Security Council Open Debate on Cyber Security; Yuval Shany and Michael N. Schmitt (2020): An International Attribution Mechanism for Hostile Cyber Operations, in: International Law Studies 96, pp. 196-222; Jason Healey, John C. Mallery, Klara Tothova Jordan, and Nathaniel V. Youd (2014): Confidence-Building Measures in Cyberspace. A Multistakeholder Approach for Stability and Security, Atlantic Council; and John S. Davis II, Benjamin Boudreaux, Jonathan William Welburn, Jair Aguirre, Cordaye Ogletree, Geoffrey McGovern and Michael S. Chase (2017): Stateless Attribution: Toward International Accountability in Cyberspace, RAND Corporation.

16 Also, scholarly contributions on attribution do, so far, not comprehensively link the practice of attributing cyber operations to normative expectations about appropriateness or approach them from a comparative perspective. A notable exception is a study by UNIDIR, which looks at attribution from a non-escalation angle and includes "suggestions of […] how to operationalize" cyber norm (b) (Andraz Kastelic (2022): Non-Escalatory Attribution of International Cyber Incidents: Facts, International Law and Politics, United Nations Institute for Disarmament Research).

17 UNGA (2021): Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security (A/76/135).

18 For example, Sven Herpig (2021): Die Beantwortung von staatlich verantworteten Cyberoperationen, Stiftung Neue Verantwortung.

19 For example, Belgium set up an attribution mechanism (UN Security Council (SC) (2021): Letter dated 1 July 2021 from the President of the Security Council addressed to the Secretary-General and the Permanent Representatives of the members of the Security Council (S/2021/621)) and Estonia adopted cyber-specific public attribution guidelines, for example, establishing an inter-agency working group in January 2019 (Ministry of Foreign Affairs Estonia (2020): Attribution and Deterrence in Cyberspace).

20 For example, Permanent Mission of Thailand to the United Nations (2023): Statement by Mr. Krirkrit Ponlakhetpaiboon […], Agenda item 5: Discussions on substantive issues contained in paragraph 1 of General Assembly resolution 75/240 on how international law applies to the use of information and communications technologies by States at the fourth substantive session of the UN OEWG 2021-2025.

perceive the normative framework in this respect. It also allows the examination of similarities and differences and thus provides indications as to whether the analyzed practices have given rise to convergence—shared understandings—about the responsible conduct of OPPA. Such convergence is desirable, as it can contribute to the development of collective expectations regarding appropriate courses of action and, in turn, guide state behavior. A comprehensive understanding of what states consider to be an (in)appropriate OPPA may contribute to preventing misunderstandings and is therefore essential for conflict prevention, conflict management, and further stabilization instruments, such as confidence-building measures.

This paper highlights the OPPA practice of four focus countries: Australia, Germany, Japan, and the U.S. These states have been selected because they have already undertaken numerous attributions and thus provide a broad basis for analysis. This selection also allows to analyze practices in different regions of the world with different policy postures and capabilities. All these states belong to the "Western" camp and therefore presumably share similar normative ideas as like-minded states. Nonetheless, "two governments will never be exactly the same in their factors to consider"[21] when engaging in OPPA.

This analysis first develops a definition of OPPA and sheds light on what is known about the four selected states' national decision-making processes for conducting OPPAs. In the following, based on their past OPPA practices, it proposes and applies an analytical framework comprising 13 parameters and corresponding options at a state's disposal when conducting OPPAs. These parameters relate to both procedural and organizational factors, as well as their communication as such. In a subsequent step, under the assumption that states may also be interested in sharing and disseminating preferences with other states, this paper analyzes whether and how the selected countries have engaged in efforts to spread their perspectives on public attribution among other states. The Annex includes country-specific lists of all OPPA practices and tabular "OPPA Profiles" based on the parameters and options introduced in Chapter 3.

In doing so, this analysis seeks to facilitate convergence of understandings on responsible OPPA. It does not attempt to prescribe what form responsible OPPA should take or what normative understandings should be established. Rather, by providing a framework that may inform both states and policymakers already engaged in public attribution and those who are not, it seeks to enhance the understanding of the options that states have at their disposal when publicly communicating a political attribution in an effort to stimulate a strategic debate on this important policy instrument.

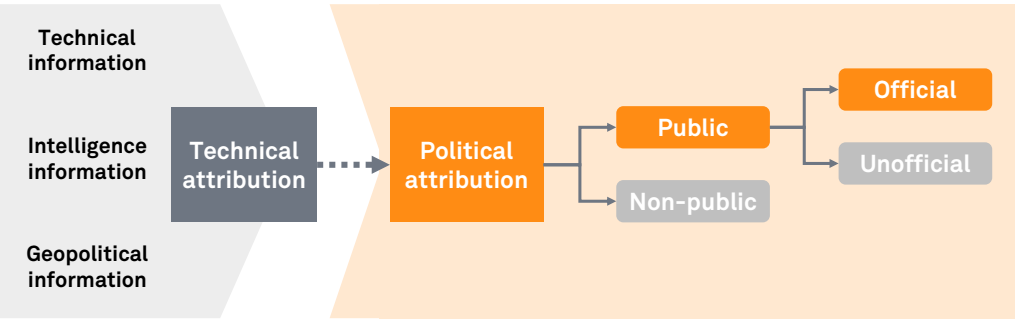
21 Florian Egloff and Max Smeets (2021): Publicly attributing cyber attacks: a framework, in: Journal of Strategic Studies 46 (3), pp. 502-533.

2. Official Public Political Attribution

2.1 Definition

This analysis examines OPPAs that are understood as a government entity's public disclosure of information tying cyber operations to another state through official channels.

Figure 1: Official Public Political Attribution



Attribution "refers to identifying the entity responsible for a cyber [operation or set of cyber operations]."[22] The focal point of attributions are cyber operations, which are defined as the "targeted use and [modification] of digital code by any individual, group, organization or state using digital networks, systems and connected devices [...] to steal, alter, destroy information or disrupt and deny functionality with the ultimate aim to weaken and/or harm"[23] specific actors. States, IT security companies,[24] and third parties, such as academic research institutions, NGOs, and the media,[25] can conduct attributions. Conceptually, attribution takes the form of technical,[26] political, and/or legal[27] attribution.[28]

22 Kristen Eichensehr (2020): The Law & Politics of Cyberattack Attribution, in: UCLA Law Review 67, pp. 520-598. A set of cyber operations can also be referred to as a cyber campaign.

23 Sven Herpig (2016): Anti-War and the Cyber Triangle: Strategic Implications of Cyber Operations and Cyber Security for the State.

24 For example, Microsoft (2023): Iran responsible for Charlie Hebdo attacks.

25 For example, Hakan Tanriverdi, Florian Flade, and Lea Frey (2022): The Elite Hackers of the FSB and John Scott-Railton, Elies Campo, Bill Marczak et al. (2022): CatalanGate Extensive Mercenary Spyware Operation against Catalans Using Pegasus and Candiru.

26 "Technical attribution determines who performed a cyber incident based on IT forensic evidence and technical traces left behind" (EuRepoC (n.d.): Glossary). Insights permitting such forensic analysis can, for example, be gained not only from affected IT systems but also through the exchange of information with other actors, including technical communities, threat intelligence companies, and foreign security agencies (Sven Herpig (2021): Die Beantwortung von staatlich verantworteten Cyberoperationen, Stiftung Neue Verantwortung).

27 In a legal sense, attribution of responsibility constitutes the "operation of attaching a given action or omission to a State" (International Law Commission (2001): Draft articles on Responsibility of States for Internationally Wrongful Acts, with commentaries) when either national or international law is being contravened. The latter only comes into play "when the entity that directs [the cyber operation(s)] is a state" (Kristen Eichensehr (2020): The Law & Politics of Cyberattack Attribution, in: UCLA Law Review 67, pp. 520-598). The attribution of legal responsibility for a cyber operation may also include a political attribution when a causal link to a political actor is established.

28 For example, Herbert Lin (2016): Attribution of Malicious Cyber Incidents. From Soup to Nuts, Hoover Institution. See also Sven Herpig (2021): Die Beantwortung von staatlich verantworteten Cyberoperationen, Stiftung Neue Verantwortung.

This analysis focuses on **political attribution**, which generally denotes the attribution of authorship for cyber operations to a specific state. It considers cases of OPPA in which the attributed political actor is another state that is being specifically mentioned within the OPPA. It excludes attributions where, for example, an unspecified nation-state is exclusively named as the perpetrator of cyber operations without further indication. An example of such a political attribution falling outside the scope of this analysis represents a 2018 statement by former Australian Prime Minister Scott Morrison, in which he stated that "Australian organisations [were] currently being targeted by a sophisticated state-based cyber actor."[29]

The attribution of a cyber operation to a particular state can come at different "levels of granularity,"[30] with the most "advanced level [being] the identification of specific organizations and individuals."[31] Attribution to a state may also extend to activities of non-state actors in instances when they act in complete dependence of another state or under its instruction, direction, or control.[32] Such actors could include mercenaries or organized crime groups. It also encompasses Advanced Persistent Threat (APT) groups. Since APTs are "typically state-controlled,"[33] an exclusive reference to an APT group may also reflect a political attribution. This analysis omits public attributions that highlight the activities of non-state actors, such as cyber crime groups or hacktivists, when no link to another state is being drawn, and the operation is thus not attributed to a specific state.[34]

It is a state's discretion whether to share a political attribution at all, and, if so, whether to use non-public or public means to that end. For instance, non-public avenues may take the form of summoning a country's ambassador, delivering a démarche, or expelling foreign diplomats. China, for instance, is reported to have been "advancing [attributions] privately at diplomatic summits, particularly in response to Western criticisms about its espionage campaigns."[35] Opposed to non-public attribution, **public** attribution means that the attribution assessment is shared in a publicly accessible way. Such publicly accessible ways can take the form of statements, publications, or reports. Public political attributions are thus likely only a fragment of total political attributions and a temporary snapshot, as many political attributions are only made after a sometimes significant period of time. States may be reluctant to go public, for instance, because it bears the risk of

29 Department of the Prime Minister and Cabinet (2018): Statement on malicious cyber activity against Australian networks. See also ACSC (2016): ACSC Threat Report 2016.
30 Timo Steffens (2020): Attribution of Advanced Persistent Threats. How to Identify the Actors Behind Cyber-Espionage, Springer-Verlag.
31 Timo Steffens (2020): Attribution of Advanced Persistent Threats. How to Identify the Actors Behind Cyber-Espionage, Springer-Verlag.
32 Art. 4 and 8 Articles on the Responsibility of States for Internationally Wrongful Acts (ARSIWA). Jason Healey (2012): Beyond Attribution: Seeking National Responsibility for Cyber Attacks, Atlantic Council.
33 BSI (n.d.): Advanced Persistent Threat.
34 As an example see Department of the Treasury (2023): United States and United Kingdom Sanction Members of Russia-Based Trickbot Cybercrime Gang.
35 Alexander Martin (12.09.2022): Beijing rebukes U.S. over alleged cyberattack on Chinese university, The Record.

losing "entry points for intelligence collection."[36] At the same time, their reluctance might also stem from wider implications. For instance, states must calculate risks for a potential misattribution that could affect their credibility. Moreover, a public attribution might influence if or the extent to which the private sector or other entities can claim insurance coverage.[37]

To exclude the possibility of states "rely[ing] on non-governmental proxies to make their accusations for them,"[38] this analysis analyzes only **official** public attributions. In contrast to non-official assessments,[39] this requires the attribution to take place via official communication channels by government entities of the attributing state. For example, it is therefore not considered an official channel when "five [unidentifiable] people with direct knowledge of the findings of the investigation"[40] are cited in a media report as the source for attributing a specific operation to another state. In practice, in addition to ministerial statements, official channels can thus take various forms,[41] comprising for instance also technical advisories or unsealed indictments, that publicly name another state as perpetrator of an operation or campaign. However, it should be noted that respective definitions of what constitutes an official channel may vary across countries given differing institutional settings and bureaucracies.

2.2 National Processes

Before discussing individual OPPA practices in the following chapter, it is essential to consider how Australia, Germany, Japan, and the U.S. reach their respective decisions. In their 2019 report, the Global Commission on the Stability of Cyberspace (GCSC) noted that "designing and exercising processes for reaching attribution at a national level and international level [...] can significantly improve the timeliness

36 Florian Egloff and Max Smeets (2021): Publicly attributing cyber attacks: a framework, in: Journal of Strategic Studies 46 (3), pp. 502-533.

37 For example, Lloyd's Market Association (2021): Cyber War and Cyber Operation Exclusion Clauses; MunichRE (2023): War exclusions on the cyber market – Taking the next step; and Isabella Brunner (2023): Insurance Policies and the Attribution of Cyber Operations under International Law: A Commentary, in: New York University Journal of International Law and Politics 55, pp. 179-192.

38 Martha Finnemore and Duncan B Hollis (2020): Beyond Naming and Shaming: Accusations and International Law in Cybersecurity, in: European Journal of International Law 31 (3), pp. 969–1003 and Kerstin Zettl-Schabath (2023): Staatliche Cyberkonflikte. Proxy-Strategien von Autokratien und Demokratien im Vergleich, transcript Verlag.

39 For example, Lee refers to a case where the 2015 operation targeting the Ukrainian power grid was attributed to Russia by the U.S. Deputy Secretary of Energy. Nonetheless, other U.S. entities "subsequently commented that evidence for the attribution was not air-tight, and that the US government was not yet prepared to attribute the cyberattack" (Heajune Lee (2023): Public attribution in the US government: implications for diplomacy and norms in cyberspace, in: Policy Design and Practice 6 (2), pp. 198-216). Similarly, also French officials have 'unofficially' attributed cyber operations in the past (Alix Desforges and Aude Géry (2021): France Doesn't Do Public Attribution of Cyberattacks. But It Gets Close., Lawfare).

40 Colin Packham (16.09.2019): Exclusive: Australia concluded China was behind hack on parliament, political parties – sources, Reuters.

41 The communication channels available to states to communicate an OPPA will be explained in more detail in Section 3.1.

and effectiveness of attribution statements."[42] A similar recommendation was made in more general terms within the 2021 GGE Report.[43] Such processes are of relevance because they can facilitate inter-agency cooperation and the assignment of responsibilities[44].

Of the four states, Australia and Germany have publicly acknowledged a national attribution process, but details remain sparse given their classified nature.[45] In comparison, the U.S. has established an attribution-encompassing, but not attribution-exclusive, policy coordination process in response to significant cyber incidents.[46] This pre-existing U.S. process was codified in 2016,[47] the Australian process already in use was disclosed in 2018,[48] and Germany followed suit with the public acknowledgment of its own national attribution process in 2021.[49]

The establishment of these processes reflects the increased political importance that Australia, Germany, and the U.S. attach to the issue of (public) attribution. There is no public information about whether Japan has a similar dedicated national process in place, either for attribution specifically or, more generally, in response to significant cyber incidents. Nonetheless, the Japanese government has hinted toward a willingness to formulate a national attribution posture.[50]

42 GCSC (2019): Advancing Cyberstability. Final Report.

43 UNGA (2021): Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security (A/76/135).

44 For example, Belgium set up an attribution mechanism (UNSC (2021): Letter dated 1 July 2021 from the President of the Security Council addressed to the Secretary-General and the Permanent Representatives of the members of the Security Council (S/2021/621)) and Estonia adopted cyber-specific public attribution guidelines, for example, establishing an inter-agency working group in January 2019 (Ministry of Foreign Affairs Estonia (2020): Attribution and Deterrence in Cyberspace).

45 But, both Australia and Germany have publicly shared insights into their processes (Regine Grienberger (2023): Cyberangreifer benennen, globale Normen stärken: Erfahrungen mit dem Attributionsverfahren der Bundesregierung, Bundesakademie für Sicherheitspolitik and Australian Foreign Affairs, Defence And Trade Legislation Committee (2021): Thursday, 3 June 2021, Official Committee Hansard).

46 This process was publicized in the form of a Presidential Policy Directive (The White House (2016): Presidential Policy Directive -- United States Cyber Incident Coordination and The White House (2016): Annex for Presidential Policy Directive -- United States Cyber Incident Coordination).

47 These processes were established under the Obama Administration in 2016 and have remained in place since (for example, The White House (2021): Executive Order on Improving the Nation's Cybersecurity).

48 Australian Foreign Affairs, Defence And Trade Legislation Committee (2019): Thursday, 24 October 2019, Official Committee Hansard.

49 In a personal opinion piece, German Cyber Ambassador Regine Grienberger alluded that the German national attribution process was the result of three developments: (a) various cyber operations having directly affected Germany, which thereby created political momentum, (b) the desire on the part of the domestic intelligence agency, police, and cybersecurity experts to publicize increasing activity of foreign intelligence services in Germany, as well as (c) the 2021 GGE Report. Building upon the inclusion of foreign and security policy considerations and the involvement of relevant authorities, Grienberger states that the German process is based on norm (b) (Regine Grienberger (2023): Cyberangreifer benennen, globale Normen stärken: Erfahrungen mit dem Attributionsverfahren der Bundesregierung, Bundesakademie für Sicherheitspolitik).

50 National Security Council Japan (2021): サイバーセキュリティ戦略案の作成に際しての国家安全保障会議意見.

All three processes place emphasis on ensuring inter-departmental coordination and designating responsibilities to that end. The processes are explained in more detail below:

Overview of Australian, German, and U.S. processes[50]

🇦🇺 The Australian national attribution process[52] aims to "guide and inform a decision by the Australian Government to make a public or private attribution disclosure."[53] It represents a joint policy of the Australian Departments of Foreign Affairs (DFAT), Home Affairs, and Defence, co-led by the two former departments.[54] In June 2021, Australia's inaugural Ambassador for Cyber Affairs and Critical Technology Tobias Feakin shared some insights into how the process plays out in practice. He disclosed that the process involves the gathering of intelligence from "Five Eyes partners and from other like-minded groups," which would then be assessed to "get to a case which is as far as possible beyond reasonable doubt proof of evidence."[55]

🇩🇪 Participating authorities in Germany's national attribution process, led by the German Federal Foreign Office, are the Federal Ministry of the Interior (BMI), the Federal Chancellery, and the Federal Ministry of Defence, with involvement of agencies in their purview, specifically the German domestic (BfV), foreign, and military intelligence agencies, as well as the national cybersecurity agency, the Federal Office for Information Security (BSI).[56] According to German Cyber Ambassador Regine Grienberger, the German process is composed of various steps, including the initiation of the inter-agency process; the collection of technical information by the intelligence agencies and the national cybersecurity agency, as well as simultaneous consultations by the Federal Foreign Office with allied states; the development of a proposal by the Federal Foreign Office on whether and how to respond politically; and subsequent discussion and decision made

51 Given only limited and selective public information on these processes, it is not possible to thoroughly compare elements of these processes with each other.

52 It is sometimes also referred to as Australian "attribution framework policy" (Australian Foreign Affairs, Defence And Trade Legislation Committee (2019): Thursday, 24 October 2019, Official Committee Hansard).

53 Australia further shared that the "process includes, but is not limited to, considering all relevant information, including the larger context of the event, the challenges of attribution in the ICT environment and the nature and extent of the consequences" (Australian Mission to the United Nations (2019): Australian Paper – Open Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security, September 2019).

54 Australian Foreign Affairs, Defence And Trade Legislation Committee (2019): Thursday, 24 October 2019, Official Committee Hansard.

55 Australian Foreign Affairs, Defence And Trade Legislation Committee (2021): Thursday, 3 June 2021, Official Committee Hansard.

56 Regine Grienberger (2023): Cyberangreifer benennen, globale Normen stärken: Erfahrungen mit dem Attributionsverfahren der Bundesregierung, Bundesakademie für Sicherheitspolitik.

by all involved ministries consensually.[57] Every involved ministry can initiate the process following a cyber incident in German networks of presumably international origin or following another state's request to join an OPPA. The proposal includes recommendations of whether, and if so how, the response should be communicated publicly.[58] Germany's national attribution process also comes into play when a coordinated attribution is sought at the EU level.[59]

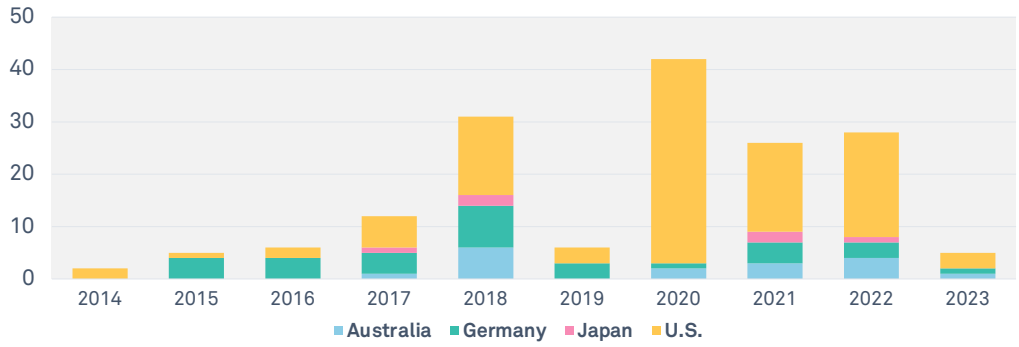
In response to significant cyber incidents, the U.S. National Security Council, under the purview of the White House and in the form of the Cyber Response Group, coordinates a policy response.[60] Under the chairmanship of a White House representative, the Cyber Response Group is composed of representatives from the State, Treasury, Defense, Justice, Commerce, Energy, and Homeland Security (DHS) Departments, as well as the United States Secret Service, the Joint Chiefs of Staff, the Office of the Director of National Intelligence (ODNI), the Federal Bureau of Investigation (FBI), the National Cyber Investigative Joint Task Force, the Central Intelligence Agency, and the NSA.[61] It is, among others, tasked with "identify[ing] and consider[ing] options for responding to significant cyber incidents, and mak[ing] recommendations to the Deputies Committee."[62] In relation to OPPA, it is also mandated to "consider the policy implications for public messaging in response to significant cyber incidents, and coordinate a communications strategy, as necessary."[63] In turn, the Cyber Response Group may involve the National Security Council's Deputies or Principals Committee for further consideration and decision, if necessary.

57 Regine Grienberger (2023): Cyberangreifer benennen, globale Normen stärken: Erfahrungen mit dem Attributionsverfahren der Bundesregierung, Bundesakademie für Sicherheitspolitik.
58 Regine Grienberger (2023): Cyberangreifer benennen, globale Normen stärken: Erfahrungen mit dem Attributionsverfahren der Bundesregierung, Bundesakademie für Sicherheitspolitik.
59 Auswärtiges Amt (2022): Jahresabrüstungsbericht 2021. Coordinated attribution at EU level will be discussed in the context of Section 3.5.
60 The White House (2016): Presidential Policy Directive -- United States Cyber Incident Coordination.
61 The White House (2016): Annex for Presidential Policy Directive -- United States Cyber Incident Coordination.
62 The White House (2016): Annex for Presidential Policy Directive -- United States Cyber Incident Coordination. The U.S. "National Security Council system" consists of four (types of) bodies, with the most-high level being the National Security Council, followed by the Principals Committee, the Deputies Committee, and multiple Interagency Policy Committees, inter alia, preparing the deliberations of their superior committees. More information on the role and tasks of the respective bodies can be found here: The White House (2021): Memorandum on Renewing the National Security Council System.
63 The White House (2016): Annex for Presidential Policy Directive -- United States Cyber Incident Coordination.

3. Official Public Political Attribution in Practice: Australia, Germany, Japan, and the U.S.

This analysis builds upon a total of 164 cases of OPPAs by the four focus countries: 109 by the U.S.,[64] 32 by Germany (including practices by the European Union (EU) in the name of EU Member States),[65] 17 by Australia, and 6 by Japan. The earliest occurred in 2014 by the U.S., followed by Germany in 2015, and Australia and Japan in 2017.[66] The cases studied in this analysis were communicated between May 2014 and May 9, 2023. To the best of the authors' knowledge, these 164 cases encompass all public attributions that match the previously introduced OPPA definition and were made by the selected countries in this specific timeframe.

Figure 2: Number of OPPAs per Year per Country



The practices of the focus countries indicate that when opting for an OPPA, states face three principal questions: (1) **what** to attribute, (2) **how** to attribute, and (3) **why** to attribute the respective cyber operation(s).

64 On the U.S. approach to public attribution see also Heajune Lee (2023): Public attribution in the US government: implications for diplomacy and norms in cyberspace, in: Policy Design and Practice 6 (2), pp. 198-216. Chris Jaikaran (2023): Cybersecurity: Selected Cyberattacks 2012-2022, Congressional Research Service includes a selective list of past U.S. attributions of nation-state activity. For a comparison of U.S. practice of attribution by indictment and EU sanctions practice see also Takashi Seto (2023): パブリックアトリビューションの「拡散」と「多様化」– 政策当局間の「多様化」の国際比較研究 –.

65 On Germany's approach to public attribution see also Rebecca Beigel (2022): Attribution von Cyberoperationen – Deutschlands öffentliche Zuschreibungen, in: Kerstin Zettl, Sebastian Harnisch, and Mischa Hansel (eds.): Asymmetrien in Cyberkonflikten. Wie Attribution und der Einsatz von Proxies die Normentwicklung beeinflussen, Nomos. Section 3.5 also discusses how the German national attribution process relates to EU attributions.

66 All cases are listed in the Annex. This analysis only includes attribution practices of the communication channel that was first used to communicate the political attribution of a specific attribution. It also includes the simultaneous, coordinated use of multiple communication channels in close temporal proximity. In these cases, each communication channel used is counted as an attribution practice. It can also encompass communication channels that extend the scope of previously attributed activity. It excludes, for example, the use of retrospective communication channels confirming already previously made attributions. An example falling outside the scope thus represents the German arrest warrant following the 2015 "Bundestag hack" as the operation had already previously been attributed to Russia. When several unrelated operations are attributed in the context of the same report, they are counted as multiple OPPAs. In contrast, if a state attributes multiple operations to another state, for example, a pattern of behavior or campaign, in one statement, this is counted as one OPPA practice.

In examining their practices, 13 parameters can be identified that reflect how the four countries have addressed these questions. These parameters relate to both procedural and organizational factors, as well as to their communication. This analysis can only account for parameters that became visible in individual OPPA practices, meaning only those that were shared externally by states. Therefore, it cannot be precluded that states may also consider these parameters for other purposes, such as strategic communication and signaling. As a matter of course, also different parameters, such as the general state of the relationship between attributing and attributed state, may play a role in internal deliberations and reasoning.[67]

When analyzing which parameters and options play a role in focus countries' OPPAs, the following six conclusions can be drawn:

Table 1: Overview of Conclusions and Parameters

Parameters	Conclusions
 Choice of communication channel	**3.1 Communication channels and designated government entities vary across countries and over time.**
 Selection of government entity(ies) communicating the OPPA	
 Factual description of the operation attributed	**3.2 OPPAs always provide details on the operations attributed.**
 Provision of details on the attributed actor	**3.3 OPPAs differ in how they specify the attributed actor and sometimes include a message addressed to the actor.**
 Inclusion of a message to the attributed actor	

67 How states address these parameters and what specific options they decide on may also be impacted by other factors outside of the scope of this analysis. For instance, given that OPPAs are inherently a public communication practice, a state's preferences may also be constrained by language particularities that can pre-determine or influence the scope for respective policy action.

Parameters	Conclusions
 Provision of or reference to evidence	**3.4 Only some OPPAs mention evidentiary information and estimative probability.**
 Inclusion of estimative probability	
 Engagement in international cooperation and coordination efforts	**3.5 States increasingly coordinate their OPPAs with like-minded countries.**
 Specification of the severity of the operation attributed	**3.6 States regularly explain why they attribute, pointing to the operation, their policies, and/or international commitments.**
 Formulation of policy objectives pursued with OPPA	
 Linkage to national (attribution) policy	
 Inclusion of reference to prior OPPAs	
 Reference to UN cyber norms or other commitments	

In acting on these parameters, states face various options reflecting a spectrum of choices. The subsequent sections explain the conclusions in detail. Each section contains tabular overviews including both parameters and options, indicating

whether a particular state has done so (●) or not (○),[68] and concludes with a dedicated section outlining the scope and implications for convergence among the focus countries. The Annex includes four country-specific "OPPA Profiles" summarizing how each focus country has considered individual parameters in its OPPA practices.

As Germany, Australia, and Japan have publicly attributed much fewer cyber operations than the U.S., their OPPA policies are likely of a more emerging nature, in contrast to a rather established U.S. approach. Yet, states will only engage in OPPAs when it is in their national interest to do so and the OPPA in question offers a political benefit. Fewer OPPAs by the other focus countries may thus also be explained by different situations in which states find themselves, such as general affectedness by cyber operations or the scope of available intelligence information to substantiate the pursuit of an OPPA. Given these considerations, and especially given the high quantitative variation of OPPAs among focus countries, the following study of their practices seeks to provide an overview that is not meant to indicate that particular options are "right" or "wrong" to pursue.

3.1 Communication channels and involved government entities vary across countries and over time.

Who participates in the decision-making process behind an OPPA and is responsible for its communication represents a foundational parameter that is closely connected to the selection of channels used to communicate an OPPA. They are essential because both may pre-determine or influence how many other parameters will be addressed—for example, the amount of factual explanation provided and the specification of reasons why an OPPA is pursued. At the same time, these two parameters are predominantly of a domestic and institutional nature.

The four focus countries have used channels[69] as a means to communicate an OPPA and have designated government entity(ies) as follows:

68 Guided by the effort to provide a general overview, these tables do not make any claims about the frequency with which states have included the respective options within their OPPAs. When Germany has done so exclusively via an EU declaration, this row indicates so by including a blue *.

69 These types also correspond to the forms that Eichensehr previously identified for the U.S. attribution practice (Kristen Eichensehr (2020): The Law & Politics of Cyberattack Attribution, in: UCLA Law Review 67, pp. 520-598). Conceivable is also the use of social media channels by high-level policymakers as a means to communicate an OPPA. To the best of the authors' knowledge, none of the focus countries has used their social media channels as the first and primary way to communicate an OPPA. But, focus countries have used their social media presence to further disseminate their OPPA previously communicated via other channels (for example, MOFA of Japan (21.12.2018), X or Marise Payne (19.02.2022), X).

Table 2: Choice of Communication Channel & Designation of Government Entity(ies) Communicating the OPPA —Options and Focus Countries' Practice

Parameter	Options	🇦🇺	🇩🇪	🇯🇵	🇺🇸
OPPA Choice of communication channel	Choice of technical communication channel	●	●	●	●
	Choice of political communication channel	●	●	●	●
	Choice of criminal law or economic sanctions channel[70]	○	○	○	●
	Combination of various communication channels as part of a coordinated attribution practice	●	○	●	●
Selection of government entity(ies) communicating the OPPA	Designation of Ministry of Foreign Affairs, national cybersecurity/ intelligence/law enforcement agency, or another government entity as communicator of the OPPA	●	●	●	●
	Joint issuance of an OPPA by multiple domestic authorities	●	○	●	●

Which channel is being selected and which domestic entities are involved can impact the framing of the OPPA and its external reception. Framing and reception can, for example, be influenced by associated policy fields as well as the purview and level of the designated entity within the political hierarchy. In addition, how states act upon these parameters can reflect the pursuit of different policy objectives[71] and the addressing of various target audiences, ranging from the attributed actor, over the international community as a whole, to the domestic public. Additionally, practical considerations can play a role, as particular channels and government entities can generate a higher degree of public spotlight than others, which may or may not be desired on the part of the attributing state.[72]

Communication Channels

The focus countries have used technical, political, criminal law, and economic sanctions channels to communicate an OPPA.[73] This analysis takes into account that

70 While separate channels in nature, the criminal law and economics sanctions channels are considered together in this option as the U.S. is the only focus country having used either channel to convey an OPPA.

71 The objectives specifically alluded to within focus countries' OPPAs are analyzed in more detail in the framework of Section 3.6.

72 For example, a ministerial statement by a country's Ministry of Foreign Affairs is highly likely to attract greater media attention than an OPPA published via a technical advisory.

73 In comparing these specific parameters and their usage by focus countries, it must be noted that not all states are in equal positions. This is because not all types of channels may be available to every state. For instance, this can be for legal reasons, as, a country's legal system may not provide the option to indict individuals acting on behalf of foreign nation-states. Or, as a matter of capacity, states may not find themselves in a position to use technical channels when desiring to communicate an OPPA that usually requires the publication of technical analysis.

an OPPA can be stand-alone, but may also be made in the framework of other policy instruments.[74] Technical, criminal law, and sanctions channels fall inside the scope of this analysis when they include information tying an operation to another state as its perpetrator.[75] Having these channel types in mind throughout the further analysis of parameters is helpful, as it permits a better analytical distinction between various OPPAs, especially given their varying objectives and the prioritization of particular aspects.

Technical channels entail alerts, advisories, and reports of a more technical nature. In focus countries' practice, they have included, for instance, annual intelligence reports by the intelligence service of a state[76] or more ad hoc alerts by a country's cybersecurity agency.[77] Technical channels are usually predominantly addressed toward domestic organizations, such as small and medium-sized enterprises or critical infrastructure entities. They can be pursued with the objective of issuing a warning before the highlighted operation or providing advice to mitigate or confine possible compromises.

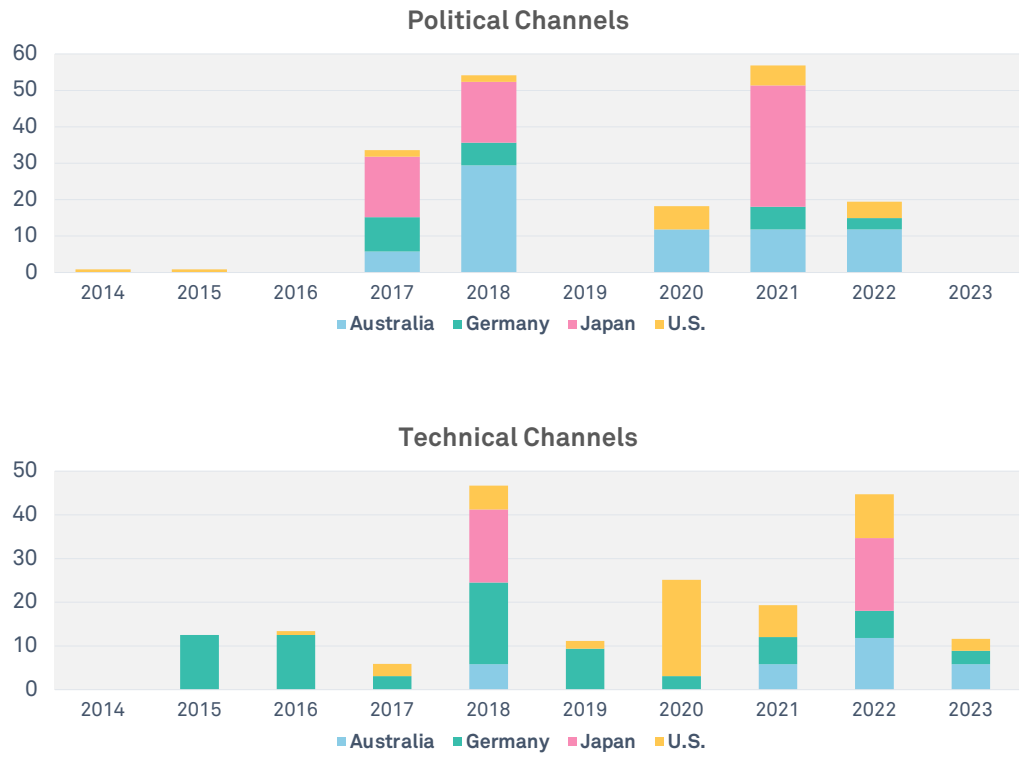
In contrast to technical channels, **political channels**[78] are usually issued by government entities at a higher political level. Examples are statements by a country's Ministry of Foreign Affairs[79] or a ministry spokesperson in the form of a press conference or press briefing,[80] the provision of an official quote for media reporting,[81] or the response to a parliamentary inquiry.[82] Political channels for publicizing an OPPA are predominantly directed toward the general public, the attributed actor, and the international community as a whole. They can serve the objectives of seeking to deter continued or future malicious behavior through its exposure or represent a strive to attain accountability for the operation attributed.

74 Sven Herpig (2021): Die Beantwortung von staatlich verantworteten Cyberoperationen, Stiftung Neue Verantwortung.
75 Hence, for example, while the criminal law channel also entails a legal attribution to an individual or organization that would generally fall outside the scope of this paper, they are considered nevertheless when a particular nexus to state involvement is drawn that also reflects a political attribution as previously defined.
76 For example, BMI (2016): Verfassungsschutzbericht 2015.
77 For example, CISA (2022): Iranian Government-Sponsored APT Actors Compromise Federal Network, Deploy Crypto Miner, Credential Harvester.
78 It must be noted that both quotes and response to a parliamentary inquiry have only been used by Germany as a means to officially attribute a cyber operation to another state for the first time.
79 For example, DFAT (2022): Attribution to Russia for malicious cyber activity against European networks.
80 For example, National Police Agency (2021): 国家公安委員会委員長記者会見要旨.
81 For example, dpa (2017): Geheimdienste: Putin ließ US-Wahl durch Hacker beeinflussen.
82 For example, German Bundestag (2017): Antwort der Bundesregierung auf die Kleine Anfrage: Ermittlungen zu angeblich russischen Cyberangriffen (Drucksache 18/11106).

Criminal law and economic sanctions channels[83] as included in this analysis are press releases of unsealed indictments and announcements of adopted sanctions.[84] They are primarily directed toward the attributed actor, but may also signal the possibility of consequences for states engaged in activities similar to the indicted or sanctioned behavior.

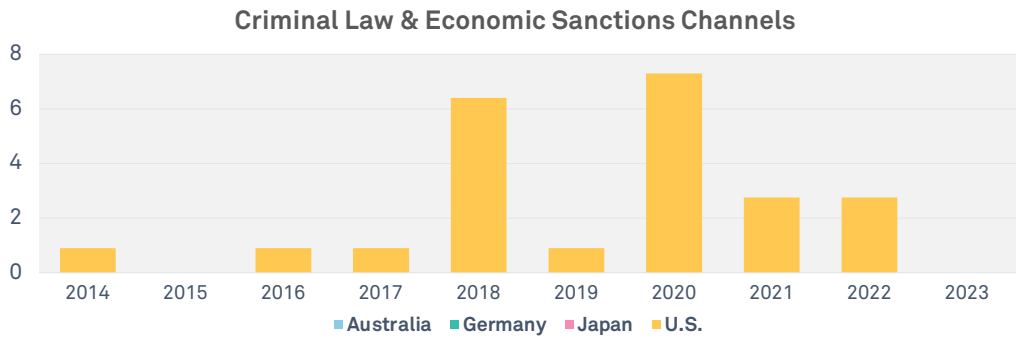
The following charts highlight the channels that the focus countries have used over the time frame analyzed to communicate an OPPA (in each case, as a percentage of a country's total OPPA practices). Annex I-IV include tabular overviews listing the respective channels used by the four states.

Figure 3: Channels Used by Focus Countries to Communicate an OPPA 2014-2023, as a Percentage of Total Practices



83 The White House and other U.S. entities have no insight into potential initiatives by the DOJ to pursue an indictment, given the separation of powers. Further along the process, the DOJ may give a heads up to different entities regarding a reached indictment. This is different to sanctions, which the Department of Treasury may be told to work on by entities of the U.S. Executive Branch. On indictments as a means for public attribution see also John P. Carlin (2016): Detect, Disrupt, Deter: A Whole-of-Government Approach to National Security Cyber Threats, in: Harvard National Security Journal 7, pp. 391-436; Garrett Hinck and Tim Maurer (2020): Persistent Enforcement: Criminal Charges as a Response to Nation-State Malicious Cyber Activity, in: Journal of National Security Law and Policy 10, pp. 525-561; and Chimène I. Keitner (2019): Attribution by Indictment, in: AJIL Unbound 113, pp. 207-212.

84 Given this paper's focus on the public communication of political attributions, for which the DOJ drafts respective press releases, and to permit better comparability across cases (because indictments generally originate from different grand juries), the scope of analysis is limited to the respective press releases announcing the unsealing of indictments, in contrast to looking additionally at the unsealed indictments as such. It is acknowledged that, in practice, the unredacted components of indictments constitute an important addition to press releases, for example, because the evidence presented permits external parties to analyze the specific incident in more detail.



Of all three channel types and across countries, technical channels were employed most frequently and by all states. Technical channels were used particularly often by the U.S. and by Germany before establishing its national attribution process in 2021. In contrast, Australia and Japan have preferred political channels. Concurrently, the Australian, German, and Japanese OPPAs display a diversification of channels used over time. For example, Australia and Japan recently began also using technical channels, whereas Germany, moving in a somewhat opposite direction, has increasingly emphasized political channels. Criminal law and economic sanctions channels have only been used by the U.S. as a means to communicate a political attribution publicly.

Coordinated OPPAs

In addition to using channels individually, focus countries have increasingly combined various channels as part of a domestically coordinated attribution practice. An OPPA practice is assumed to be domestically coordinated when different communication channels are used simultaneously on the same day or in very close temporal proximity. This has included the combination of technical and political channels or the use of the same channel type by two different entities. The respective OPPAs usually, but not always, referenced each other.[85] The analysis showed that 32% of U.S. OPPAs have been issued simultaneously via various channels. Starting in 2020, the U.S. has also practiced public attribution via all three types of channels simultaneously in four instances. Australia and Japan have also each published a corresponding alert to an attribution via political channels once.[86]

85 For example, The White House (2021): Fact Sheet: Imposing Costs for Harmful Foreign Activities by the Russian Government and DOJ (2022): Four Russian Government Employees Charged in Two Historical Hacking Campaigns Targeting Critical Infrastructure Worldwide.

86 Ministry of Foreign Affairs of Japan (2018): Cyberattacks by a group based in China known as APT10 (Statement by Press Secretary Takeshi Osuga) and ACSC (2018): Routers targeted: Cisco Smart Install feature continues to be targeted by Russian state-sponsored actors.

The combination of channels can impact how states act on other policy options, allowing them to emphasize various aspects by leveraging the particularities of different channels. Coordinated OPPAs can contribute to a comprehensive government response to a specific cyber operation by combining multiple tools at a state's disposal, but they require a substantial amount of dedicated resources to realize. Thus, such domestically coordinated OPPAs likely primarily represent a possibility in response to operations that are deemed particularly significant and whose effects may be highly palpable at the time of the OPPA's communication.

Selected Government Entities

Regarding who is designated to publish an OPPA via any of these channels reveals a considerable spectrum ranging from three (Germany), four (Japan), six (Australia) to 14 (U.S.) entities having previously communicated OPPAs.[87] This is unsurprising given different jurisdictional contexts and does not (necessarily) account for other domestic entities additionally involved pre-OPPA in collection, analysis, or decision-making. Ministries of Foreign Affairs, national cybersecurity agencies, and intelligence agencies of the focus countries were particularly often involved in the communication of an OPPA. Annex I-IV list all attributing actors per focus country and OPPA.

In the Australian[88] and Japanese cases, their Ministries of Foreign Affairs were the most visible players in the communication of their attributions, as has been the case for Germany since 2021. In Japan, the Japanese National Police Agency increasingly surfaced as an OPPA actor, having been involved in OPPAs twice—one-third of Japanese total OPPAs—since 2021. Similar to Australia, Japan, and Germany, the U.S. State Department issued most of the U.S. OPPA's through political channels. Yet, when looking at the total U.S. OPPA practices across all three channels, the U.S. State Department—unlike the other states—has only acted as a communicator in roughly 13 % of U.S. OPPAs. The FBI and the Cybersecurity and Infrastructure Security Agency (CISA)/DHS are the three U.S. entities that have most often publicized an OPPA.

Joint OPPAs

The practices of the focus countries indicate that attribution is increasingly seen as an issue demanding inter-agency cooperation. For instance, multiple domestic authorities of the U.S. and Australia jointly issued OPPAs and, more recently, Japan[89]

87 All entities are counted as separate actors. Thus, those entities that operate within the purview of another governmental entity are not consolidated as one actor.

88 In Australia, as outlined in Section 2.2, whether and how to attribute is a joint Foreign Minister and Home Affairs Minister role in conjunction with the Minister of Defence.

89 Germany's attribution practices have so far continuously been published by individual ministries or agencies, but their national process since 2021 foresees prior consultation with other domestic entities.

did the same. For the U.S., this has become visible especially in the form of technical channels[90] and for Australia through statements.[91] In this regard, it is noteworthy that roughly 90 % of U.S. attributions in the form of alerts, advisories, or reports, and 58 % of Australian OPPAs via ministerial statements were issued by more than one ministry/domestic agency. The latest Japanese OPPA via alert dating from October 14, 2022 represents the first concerted effort by Japanese agencies.[92] In contrast, Germany has exclusively communicated OPPAs through individual entities.

Convergence among Focus Countries
Of all the parameters discussed, the selection of communication channels and the designation of government entities are the parameters that most depend on domestic political considerations and the institutional set-up of a particular state. Given the broad variation in both channels and government entities involved in communicating OPPAs, substantial international convergence on these matters is limited. The practices of the four countries in question indicate that these decisions rest on specific national peculiarities. Whether states pursue domestically coordinated or conjoint OPPAs is most likely pre-determined by varying institutional designs and mandates in different states

3.2 OPPAs always provide details on the operations attributed.

Determining what has happened constitutes the central object of any OPPA and can lay the groundwork for providing a line of argumentation as to why public attribution is being pursued in a particular instance. It thus represents a fundamental parameter that all focus countries have acted on in the affirmative within their OPPAs. Yet, what details are provided on an operation depends heavily on what actually took place or is known about it. More importantly, it is up to a state to decide what and how much details to share publicly in this respect.

90 While constellations of authoring entities vary, there have been repeated joint efforts by the DHS, FBI, and Department of Defense (DoD); CISA and FBI; and DHS and FBI. Other constellations used in more than once incident are joint publications by CISA, FBI, and NSA as well as the DHS, FBI, and the Treasury Department.

91 Since 2021, the most frequent combination of Australian actors issuing a public attribution was composed of the Minister for Foreign Affairs, the Minister for Home Affairs together with the Minister for Defence. Individual statements were issued in the period of 2017-2020 twice each by the Minister for Foreign Affairs and the Minister for Law Enforcement and Cyber Security. According to a representative of the Department of Home Affairs of Australia, such a conjoint domestic approach for communicating attributions was – as of June 2021 – also representing the Australian "Prime Minister's preference" (Australian Parliamentary Joint Committee on Intelligence and Security (2021): Friday, 11 June 2021, Official Committee Hansard). Yet, it was left open what the exact impact of this preference entails in practice.

92 The alert was jointly issued by the Japanese National Police Agency, the Japanese National Center of Incident Readiness and Strategy for Cybersecurity (NISC), and the Japanese Financial Services Agency (National Police Agency, Financial Services Agency & National Center of Incident Readiness and Strategy for Cybersecurity (2022): 北朝鮮当局の下部組織とされるラザルスと呼称されるサイバー攻撃グループによる暗号資産関連事業者等を標的としたサイバー攻撃について（注意喚起）).

Focus countries have touched upon the following aspects in their descriptions of the operations attributed:

Table 3: Factual Description of Operation Attributed—Options and Focus Countries' Practice

Parameter	Options	🇦🇺	🇩🇪	🇯🇵	🇺🇸
Factual description of the operation attributed	Indication of (type of) target/victim and/or its location	●	●	●	●
	Indication of date when the operation attributed took place and, if applicable, its duration	●	●	●	●
	Indication of harm and/or damage caused by the operation attributed	●	●	○	●

Their practices indicate that states have some leeway when it comes to what and how much they share. What elements of an operation a state chooses to emphasize in the framework of an OPPA can also influence other parameters. Of all the focus countries, Japan has been the least explicit when it comes to outlining what has happened. The others mostly include information on at least two, if not all three, options.

Relating to the operation attributed, focus countries have usually provided information on the **target and/or victim of the operation**. States have, inter alia, adduced that critical infrastructure entities[93] or government actors[94] have been among the targets and emphasized in which area or sector the affected entities work or have specialized in, for example, "COVID-19-related research."[95] Other targets highlighted in focus countries' OPPA include media and broadcasting entities,[96] "sporting institutions,"[97] businesses,[98] NGOs,[99] think tanks,[100] and academic and research institutions.[101] Also, managed service[102] and "web hosting providers"[103] have been named as specific targets.

93 Among the sectors particularly mentioned in focus countries' OPPA feature the banking/financial, transportation, energy, and healthcare sector.

94 For example, Germany mentioned that its Federal Chancellery and the Federal Financial Supervisory Authority were among the targeted entities (BMI (2015): Verfassungsschutzbericht 2014). Australia once mentioned in its statement that "websites affected included sites belonging to the Georgian government" (DFAT (2020): Attribution of malicious cyber activity in Georgia by Russian Military Intelligence).

95 CISA (2020): FBI-CISA PSA PRC Targeting of COVID-19 Research Organizations. In addition, for example, in an alert Germany referred to "Wirtschaft und Forschung im Bereich Energietechnik, Röntgen- und Nukleartechnologie, Messtechnologie, Luft- und Raumfahrt sowie Rüstung" [business and research in the fields of energy technology, X-ray and nuclear technology, measurement technology, aerospace and armaments, own translation] (BfV (2016): BfV Cyber-Brief Nr. 02/2016) as being in particular interest of the attributed actor, Snake, in this instance.

96 For example, DFAT (2020): Attribution of malicious cyber activity in Georgia by Russian Military Intelligence.

97 For example, DFAT (2018): Attribution of a pattern of malicious cyber activity to Russia.

98 For example, National Police Agency (2021): 国家公安委員会委員長記者会見要旨.

99 For example, DOJ (2020): Two Iranian Nationals Charged in Cyber Theft and Defacement Campaign Against Computer Systems in United States, Europe, and Middle East.

100 For example, BMI (2020): Verfassungsschutzbericht 2019.

101 For example, Ministry of Foreign Affairs of Japan (2018): Cyberattacks by a group based in China known as APT10 (Statement by Press Secretary Takeshi Osuga).

102 For example, BfV (2017): BfV Cyber-Brief Nr. 02/2017.

103 DFAT(2020): Attribution of malicious cyber activity in Georgia by Russian Military Intelligence.

States also often referred to the location of the target, for instance, by highlighting in which countries the targets were located,[104] whether domestic organizations have been among the entities targeted,[105] or if entities in allied or partner states have been affected.[106] In many instances, states have also indicated when the operation took place and partially when it began, or whether it was still ongoing,[107] thus providing details on the **timing and duration of the operation**.

In their factual descriptions, the focus countries also brought up whether the operation attributed caused any physical **harm**, such as threatening or "put[ting] lives at risk,"[108] for example, by meddling with the delivery of health treatment options.[109] Also, economic **damage**, for instance, due to "significant remediation costs"[110] for the private sector, has been alluded to by the U.S.[111]

Convergence among Focus Countries
The four focus countries seem to agree that OPPAs should always provide some details on the operation(s) attributed. In this respect, many OPPAs particularly emphasized the targets of an operation, followed by when the operation took place. Across cases, discussions of damage and harm were increasingly, but less often alluded to.

3.3 OPPAs differ in how they specify the attributed actor and sometimes include a message addressed to the actor.

Among the parameters particularly impacted by the parameters discussed in section 3.1 are how states specify the attributed actor and whether they include a message

104 For example, DOJ (2018): Nine Iranians Charged With Conducting Massive Cyber Theft Campaign on Behalf of the Islamic Revolutionary Guard Corps.
105 For example, Ministry of Foreign Affairs of Japan (2018): Cyberattacks by a group based in China known as APT10 (Statement by Press Secretary Takeshi Osuga).
106 For example, The White House (2022): Statement by NSC Spokesperson Adrienne Watson on Iran's Cyberattack against Albania.
107 For instance, Australia once included the detail that the operation attributed took place "in May this year" (DFAT (2017): Australia attributes WannaCry ransomware to North Korea), the U.S. has noted that an operation attributed "began in January 2022 prior to Russia's invasion of Ukraine" (Department of State (2022): Attribution of Russia's Malicious Cyber Activity Against Ukraine), or Germany referenced that "Angriffe fanden vermutlich zwischen August 2017 und Juni 2018 statt und dauern vermutlich noch an" [attacks likely occurred between August 2017 and June 2018 and are believed to be ongoing, own translation] (BfV (2018): BfV Cyber-Brief Nr. 02/2018).
108 The White House (2017): Press Briefing on the Attribution of the WannaCry Malware Attack to North Korea.
109 For example, the U.S. has highlighted that "the potential theft of this information jeopardizes the delivery of secure, effective, and efficient treatment options" (CISA (2020): FBI-CISA PSA PRC Targeting of COVID-19 Research Organizations).
110 The White House (2021): The United States, Joined by Allies and Partners, Attributes Malicious Cyber Activity and Irresponsible State Behavior to the People's Republic of China.
111 See also The White House (2021): Fact Sheet: Imposing Costs for Harmful Foreign Activities by the Russian Government.

addressed to it. Focus countries' OPPAs have always attributed authorship for the outlined behavior and have sometimes added a message directed at the respective political entity. In addition to a factual description of what has happened, laying out who has done it therefore represents an equally essential element of any OPPA.

Table 4 provides an overview of the details provided by focus countries on the attributed actor and messaging examples, which will be discussed in more detail below.

Table 4: Provision of Details on Actor Attributed & Message to Attributed Actor — Options and Focus Countries' Practice

Parameter	Options	🇦🇺	🇩🇪	🇯🇵	🇺🇸
Provision of details on the attributed actor	Reference to individuals working for organs or entities of a particular state	○	○	○	●
	Reference to organs or entities of a particular state	●	●	○	●
	Reference to actors operating under the direction of or sponsorship by a specific organ/entity of a particular state	●	●	●	●
	Reference to actors operating under the direction of or sponsorship by government of a particular state	●	○	●	●
	Reference to government of a particular state	●	●	○	●
	Reference to "state X"	●	○	●	●
	Exclusive reference to a specific APT group	○	●	○	○
	Additional provision of details about the location out of which the attributed actor has operated	○	○	●	●
	Additional inclusion of reference to prior activities/operations of attributed actor	●	●	○	●
Inclusion of a message to the attributed actor	Appeal to attributed actor to cease operation attributed	●	●	○	●
	Announcement of possible further consequences	○	●*	○	●

Actor Attributed

An OPPA, as defined in this analysis, attributes authorship to the government of another state.[112] In practice, the relationship between the attributed government and the perpetrator(s) of a cyber operation is best described as a "spectrum"[113] that, according to Jason Healey, ranges from "state-prohibited" to "state-integrated" non-state actors.[114] This is because, for instance, cyber criminal groups may pledge their allegiance to a specific government and conduct activities in their support[115] or government entities actively recruit private sector personnel to work for them.[116] From a technical standpoint, the leap from attributing an activity to an actor group to attributing an activity to specific individuals is one of the most challenging steps.

Given this spectrum, states have some leeway with respect to how they refer to the perpetrator of cyber operations within their OPPA. To this effect, focus countries have employed seven different ways to point out that they consider another government to be politically responsible for the cyber operation in question.

Decreasing in specificity, focus countries have referred to:

- (1) **Individuals working for organs or entities of a particular state**,
- (2) **Organs or entities of a particular state**,
- (3) **Actors operating under the direction of or sponsored by either a specific organ/entity** or (4) **the government of a particular state**,
- (5) The **government of a particular state**,
- (6) A **particular state**, or
- (7) Exclusively to an **APT group**.[117]

The Annex includes an overview of which actors have been attributed within individual OPPAs. The degree to which respective references are specified is likely the product

112 When it comes to attribution under international law, it should be noted that the law of state responsibility lays out strict rules under which circumstances acts are attributable to a state (see Chapter II, International Law Commission (2001): Draft articles on Responsibility of States for Internationally Wrongful Acts, with commentaries).

113 Jason Healey (2012): Beyond Attribution: Seeking National Responsibility for Cyber Attacks, Atlantic Council.

114 The categories in between are "(2) state-prohibited-but-inadequate [...,] (3) state-ignored [...,] (4) state-encouraged [...,] (5) state-shaped [...,] (6) state-coordinated [...,] (7) state-ordered [...,] (8) state-rogue-conducted [... and] (9) state-executed" (Jason Healey (2012): Beyond Attribution: Seeking National Responsibility for Cyber Attacks, Atlantic Council).

115 For example, Aj Vicens (25.02.2022): Conti ransomware group announces support of Russia, threatens retaliatory attacks, Cyberscoop.

116 For example, Paul Mozur and Chris Buckley (26.08.2021): Spies for Hire: China's New Breed of Hackers Blends Espionage and Entrepreneurship, The New York Times.

117 Exclusive means that the OPPA in question did not include any information matching other higher levels of specificity as outlined. For example, if the name of an APT group was mentioned in addition to any higher level, they were considered in the context of these respective levels instead.

of political preferences, underlying evidence, and the mandate of the government entity communicating the OPPA. The degree of specificity may also change over the course of a state's maturing attribution policies and capacities.

In terms of political preferences, the extent of specificity provided is relevant, as it can have different political implications. For example, suppose an attributing state's key objective in pursuing an OPPA is to deter the attributed actor from engaging in similar behavior in the future. In that case, a more specific description of the perpetrator can signal the sophistication of a state's attribution skills, which may limit the amount of room for the political leadership of the attributed state to claim plausible deniability and avoid political responsibility. Especially when coupled with an outline of the attributed actor's previous activity, enhanced specificity can also provide a more precise public record of another state's activities. At the same time, a more specific identification of the perpetrator may also make it more necessary to substantiate the attribution claim with evidence. Specifying an individual as the attributed actor can also make other measures possible, such as sanctions or arrest warrants.

Focus countries' practices indicate that levels of specificity vary depending on the channel type used for an OPPA.

Political Channels

From all channel types, political channels showed the greatest variety in how an attributed actor was specified. Both Australia and the U.S. mentioned organs or entities of a particular state,[118] actors operating under the direction of or sponsored

118 For example, the U.S. has attributed cyber operations to the "GRU [...] also known as Unit 74455 and Sandworm" (Department of State (2020): The United States Condemns Russian Cyber Attack Against the Country of Georgia) or the Chinese Ministry of State Security (The White House (2021): The United States, Joined by Allies and Partners, Attributes Malicious Cyber Activity and Irresponsible State Behavior to the People's Republic of China). Among others, Australia has attributed cyber operations to the Russian GRU (Australian Government (2022): Attribution to Russia of malicious cyber activity against Ukraine) or the Chinese Ministry of State Security (DFAT (2021): Australia joins international partners in attribution of malicious cyber activity to China).

by a specific organ/entity[119] or the government of a particular state,[120] the government of a particular state,[121] or exclusively indicated the name of a particular state.[122]

While there was no single predominant level of specificity employed by the U.S. within political channels,[123] Australian OPPA practice via ministerial statements[124] was predominantly characterized by the second highest level of specificity, namely the designation of organs or entities of a particular state. Among the attributed entities by Australia via statements are a group acting on behalf of the Chinese Ministry of State Security (MSS),[125] the Russian Main Intelligence Directorate (GRU),[126] and North Korea.[127] However, U.S. OPPA practices of the last few years also indicated a tendency towards higher levels of specificity.[128] In statements, the U.S., for instance, named the Russian GRU[129] and the Russian Foreign Intelligence Service (SVR),[130] "cyber actors affiliated with PRC's MSS,"[131] as well as the Iranian[132] and North Korean governments[133] as perpetrators of a specific cyber operation.

119 For instance, the U.S. attributed–at that level of specificity–cyber operations to "Russian military cyber operators" (Department of State (2022): Attribution of Russia's Malicious Cyber Activity Against Ukraine) or "Chinese cyber actors associated with the Chinese Ministry of State Security" (Department of State (2018): Joint Statement by Secretary of State Michael R. Pompeo and Secretary of Homeland Security Kirstjen Nielsen: Chinese Actors Compromise Global Managed Service Providers). Australia has referred to a "group known as APT10 acting on behalf of the Chinese Ministry of State Security" (DFAT (2018): Attribution of Chinese cyber-enabled commercial intellectual property theft) in the past.

120 For example, the U.S. has mentioned "cyber actors and non-traditional collectors affiliated with the People's Republic of China" (Department of State (2020): The United States Condemns Attempts by P.R.C.-Affiliated Actors To Steal American COVID-19 Research) or "state-sponsored actors, including Iranian groups" (Department of State (2021): Designation of Iranian Cyber Actors for Attempting to Influence the 2020 U.S. Presidential Election). In a similar vein, Australia has alluded to "Russian state-sponsored actors" (e.g. DFATe (2018): Australian Government attribution of cyber incident to Russia) in the past.

121 For instance, both the U.S. and Australia have attributed cyber operations to the Russian government (e.g. Department of State (2021): Holding Russia To Account, DFAT (2022): Attribution to Russia for malicious cyber activity against European networks), the U.S. also additionally to the Iranian (e.g. The White House (2022): Statement by NSC Spokesperson Adrienne Watson on Iran's Cyberattack against Albania), and North Korean governments (e.g. FBI(2014): Update on Sony Investigation).

122 For example, the U.S. once exclusively mentioned "North Korea" (The White House (2017): Press Briefing on the Attribution of the WannaCry Malware Attack to North Korea), and also in one Australian OPPA, it was only mentioned that "North Korea [would have] carried out WannaCry ransomware campaign" (DFAT (2017): Australia attributes WannaCry ransomware to North Korea).

123 North Korean entities were attributed via statements for the first time in 2014, Iranian entities in 2015, Russian actors in 2017, and Chinese actors in 2020.

124 Notably, Australian attribution practice via statements did not attribute a cyber operation to Iran to date. North Korean entities were attributed via statements for the first time in 2017 and Chinese and Russian entities in 2018.

125 DFAT (2018): Attribution of Chinese cyber-enabled commercial intellectual property theft.

126 DFAT (2020): Attribution of malicious cyber activity in Georgia by Russian Military Intelligence.

127 DFAT (2017): Australia attributes WannaCry ransomware to North Korea.

128 Annex IV includes a tabular overview of all attributed actors by the U.S.

129 The White House (2022): Press Briefing by Press Secretary Jen Psaki, Deputy National Security Advisor for Cyber and Emerging Technology Anne Neuberger, and Deputy National Security Advisor for International Economics and Deputy NEC Director Daleep Singh, February 18, 2022.

130 The White House (2021): Fact Sheet: Imposing Costs for Harmful Foreign Activities by the Russian Government.

131 The White House (2021): The United States, Joined by Allies and Partners, Attributes Malicious Cyber Activity and Irresponsible State Behavior to the People's Republic of China.

132 The White House (2022): Statement by NSC Spokesperson Adrienne Watson on Iran's Cyberattack against Albania.

133 FBI (2014): Update on Sony Investigation.

In contrast to the U.S. and Australia, German and Japanese attribution practices—in general—made use of less specific references when naming the attributed actor. In this respect, it is noteworthy that Japan never employed entity-specific references in statements by its Ministry of Foreign Affairs, either directly or indirectly through individuals or actors acting on their behalf or under their sponsorship. Instead, Japanese OPPAs via statements attributed operations either to actors or individuals acting on behalf of or under sponsorship by the government of a specific state[134] or exclusively referred to the name of the country without further indications.[135] Japanese entities other than the Japanese Ministry of Foreign Affairs attributed cyber operations to another state at a higher level of specificity. In a press conference, Japan's National Police Agency attributed an operation to the group Tick, which was argued to be an organization of the Chinese People's Liberation Army's (PLA) Strategic Support Unit Network System Department 61419,[136] indicating that the government entity issuing the OPPA may impact how the attributed actor is specified.

Among the studied cases, German OPPAs announced via political channels displayed the broadest range of invoked specificity, ranging from specific entities,[137] the government of a specific state,[138] or APT groups.[139] However, exclusive references to APT groups were last included in 2018, thereby confirming the tendency for OPPAs announced via political channels to show increased specificity.

Technical Channels

Compared to their political counterparts, focus countries have generally employed higher specificity when disclosing information about the perpetrator of a cyber operation in their usage of technical channels. For instance, Australian OPPAs communicated via technical channels referred either to actors operating under the direction of or sponsorship by a specific organ/entity[140] or the government[141] of a

134 Ministry of Foreign Affairs of Japan (2021): Cases of cyberattacks including those by a group known as APT40 which the Chinese government is behind (Statement by Press Secretary YOSHIDA Tomoyuki).

135 Ministry of Foreign Affairs of Japan (2017): The U.S. Statement on North Korea's Cyberattacks (Statement by Press Secretary Norio Maruyama). Among the entities attributed by Japan via statements are APT40, a Chinese government-sponsored group, North Korea, as well as a group "based in China known as APT10" (Ministry of Foreign Affairs of Japan (2018): Cyberattacks by a group based in China known as APT10 (Statement by Press Secretary Takeshi Osuga)). North Korean entities were attributed via statements for the first time in 2017 and Chinese entities in 2018.

136 National Police Agency (2021): 国家公安委員会委員長記者会見要旨.

137 Auswärtiges Amt (2021): Cyberangriffe auf Bundestagsabgeordnete und Landtagsabgeordnete durch den Cyberakteur „Ghostwriter".

138 Auswärtiges Amt (2022): Auswärtiges Amt verurteilt Cyberangriff der Russischen Föderation.

139 For example, the former President of the German domestic intelligence service BfV, Hans-Georg Maaßen, referred to APT28 (dpa (2017): Geheimdienste: Putin ließ US-Wahl durch Hacker beeinflussen) or the Federal Government highlighted the activity of APT29 in its answer to a parliamentary inquiry (German Bundestag (2017): Antwort der Bundesregierung auf die Kleine Anfrage: Ermittlungen zu angeblich russischen Cyberangriffen (Drucksache 18/11106)).

140 CISA et al. (2022): Iranian Islamic Revolutionary Guard Corps-Affiliated Cyber Actors Exploiting Vulnerabilities for Data Extortion and Disk Encryption for Ransom Operations.

141 CISA et al. (2021): Iranian Government-Sponsored APT Cyber Actors Exploiting Microsoft Exchange and Fortinet Vulnerabilities in Furtherance of Malicious Activities.

particular state. Similar to Australia, U.S. public attributions in the form of alerts and advisories[142] most frequently attributed operations to actors operating on behalf of or under sponsorship by the government of a specific state.[143] Especially since 2020, U.S. authorities also increasingly referenced organs or entities of a particular state[144] or actors operating under their direction or sponsorship.[145] The tendency toward increased specificity in OPPAs issued through technical channels is also displayed in the only alert that Japan has published to communicate an OPPA to date, in which it attributed authorship to the Lazarus Group, claimed to be a subgroup overseen by North Korean authorities.[146]

Germany predominantly referred to an APT group for attribution when using technical channels.[147] When doing so, two types of references can be distinguished that match different specificity levels. Which type was employed depends on which particular technical channel has been used. Whereas alerts mainly exclusively mentioned an APT or other actor group, attributions in annual intelligence or other reports were either titled or included in the framework of chapters that imply a link to specific foreign intelligence services. In contrast to the former, the latter can be equated to naming actors operating under the direction of or sponsorship by a distinct organ/entity of a particular state.[148] Once, in 2019, the German annual intelligence report also specifically attributed an operation to the Russian GRU.[149]

Criminal Law and Economic Sanctions Channels

Different from political and technical channels that offer states some political leeway, the legal underpinnings of indictments pre-determine the degree of specificity required when this channel is being pursued. The pursuit of individual, as opposed to sectoral, sanctions, may also preset the level of specificity that needs

142 North Korean entities were attributed via alerts for the first time in 2017, Russian entities in 2018, Chinese actors in 2020, and Iranian actors in 2021.

143 For example, FBI and CISA (2022): Russian State-Sponsored Cyber Actors Gain Network Access by Exploiting Default Multifactor Authentication Protocols and "PrintNightmare" Vulnerability.

144 For example, NSA et al. (2021): Russian GRU Conducting Global Brute Force Campaign to Compromise Enterprise and Cloud Environments.

145 For example, National Cyber Security Centre (2021): Joint advisory: Further TTPs associated with SVR cyber actors.

146 National Police Agency, Financial Services Agency & National Center of Incident Readiness and Strategy for Cybersecurity (2022): 北朝鮮当局の下部組織とされるラザルスと呼称されるサイバー攻撃グループによる暗号資産関連事業者等を標的としたサイバー攻撃について（注意喚起）.

147 Chinese entities were attributed via alerts for the first time in 2015, Russian and Iranian entities in 2016, and North Korean entities in 2023.

148 These attributions were made in the framework of chapters on "Spionage und sonstige nachrichtendienstliche Aktivitäten" [espionage and other intelligence activities]. In later versions of the annual intelligence reports, the caption has been adapted and also explicitly lists cyber operations, e.g. "Spionage, Cyberangriffe und sonstige sicherheitsgefährdende oder geheimdienstliche Aktivitäten für eine fremde Macht" [espionage, cyber attacks, and other security-threatening or intelligence activities for a foreign power, own translation]. Later versions of the report also cluster respective activities of intelligence and security agencies in country-specific subchapters. For example, attributions contained in these reports linked specific operations to Russian, Chinese, and Iranian intelligence services.

149 BMI (2019): Verfassungsschutzbericht 2018.

to be invoked. Respective national U.S. legislation[150] and sanctions authorities[151] necessitate an attribution at the individual level or of either an organ or entity of a particular state or actors operating under the direction of or sponsorship by either a specific organ/entity or the government of a particular state.[152] While all of these four (out of the seven) levels of specificity have been employed, U.S. OPPA practice via criminal law and economic sanctions channels has most often identified actors or individuals acting on behalf of or under sponsorship by a specific state or organ/entity of a specific state. For example, individuals working in Unit 61398 of the Chinese PLA,[153] Units 26165 and 74455 of the Russian GRU,[154] Units of the North Korean Reconnaissance General Bureau (RGB),[155] and Iran's Ministry of Intelligence and Security (MOIS), together with its Minister of Intelligence[156] were identified.

Additional Information on Attributed Actor

In addition to specifying the attributed actor, Australia, Germany, and the U.S. have also included **references to prior operations by the attributed actor** in a few instances. For example, the U.S. underlined that the "GRU's malign cyber activities include deployment of the NotPetya and Olympic Destroyer malware."[157] Corresponding references can offer the benefit of painting a comprehensive picture, increasing coherence between practices, and underlining the necessity of resorting to an OPPA in the specific incident given the outlined track record of the attributed actor. These references may also be used to tie together operations of the same campaign or to create a chain of attribution evidence. Japan has not included respective references in its OPPAs.

Lastly, two focus countries have also, albeit rarely, provided details concerning the **operating location of the attributed actor**. The U.S.[158] has done so a few times

150 For example, §1030 of the United States Code 'Fraud and related activity in connection with computers' (Office of the Law Revision Council (n.d.): United States Code). On the relationship between U.S. legislation and attribution see also Kristen Eichensehr (2021): Cyberattack Attribution as Empowerment and Constraint, Hoover Institution.

151 For example, The White House (2021): Executive Order on Blocking Property with Respect to Specified Harmful Foreign Activities of the Government of the Russian Federation.

152 This is because they speak either of "whoever" conducted outlined crimes or of "persons" who may face criminal charges or sanctions. Both can be used interchangeably and are defined as including "any individual, corporation, company, association, firm, partnership, society, or joint stock company" (§ 921 (a) (1) of the United States Code).

153 DOJ (2014): U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage.

154 DOJ (2018): Grand Jury Indicts 12 Russian Intelligence Officers for Hacking Offenses Related to the 2016 Election.

155 DOJ (2021): Three North Korean Military Hackers Indicted in Wide-Ranging Scheme to Commit Cyberattacks and Financial Crimes Across the Globe.

156 Department of the Treasury (2022): Treasury Sanctions Iranian Ministry of Intelligence and Minister for Malign Cyber Activities.

157 Department of the Treasury (2021): Treasury Sanctions Russia with Sweeping New Sanctions Authority.

158 The U.S. has, for example, highlighted that "APT40 [...] is located in Haikou, Hainan Province" (FBI and CISA (2021): Tactics, Techniques, and Procedures of Indicted APT40 Actors Associated with China's MSS Hainan State Security Department) or noted that "the charged intelligence officers [...] worked for the Jiangsu Province Ministry of State Security [...], headquartered in Nanjing" (DOJ (2018): Chinese Intelligence Officers and Their Recruited Hackers and Insiders Conspired to Steal Sensitive Commercial Aviation and Technological Data for Years).

through both technical channels and indictments, whereas Japan once included respective information in a press conference. For example, Japan specified that the Chinese PLA's Strategic Support Unit Network System Department 61419 would be based in the city of Qingdao within China's Shandong Province.[159] Including locational indications can underline a state's resolve to respond to the attributed behavior and may demonstrate its own analytical capacities.

Message to Attributed Actor

Focus countries have also included messages, with varying emphases, toward the attributed actor within their OPPAs disseminated via political channels. In this respect, all focus countries except for Japan have included **calls to cease the operation attributed or refrain from similar types of activities** in some of their OPPA practices,[160] which Australia also linked to the operation causing an inconsistency with international commitments.[161] In its statement following the Ghostwriter operation, Germany, for example, strongly urged the Russian government to end undue cyber activities immediately.[162] In the same OPPA, Germany also mentioned previous private bilateral interactions with the attributed state in which Germany raised the highlighted activities and underlined that the operation attributed would heavily impact its bilateral relationship with the attributed actor, the Russian Federation.[163] Similarly, on one occasion, the U.S. highlighted previous bilateral exchanges, specifically recounting that it "raised [its] concerns about both this incident and the PRC's broader malicious cyber activity with senior PRC Government officials."[164] Nonetheless, if included, such references may require making public preceding confidential bilateral diplomatic engagements. At the same time, they can offer attributing states the opportunity to highlight that prior measures were taken before making the attribution public.

Germany,[165] the EU, and the U.S. also used OPPAs to signal the **possibility of additional response measures in the future**. For example, the EU, in the name of all EU Member

159 National Police Agency (2021): 国家公安委員会委員長記者会見要旨.
160 For example, Minister for Law Enforcement and Cyber Security (2018): Australian Government attribution of cyber incident to Russia; Council of the European Union (2021): China: Declaration by the High Representative on behalf of the European Union urging Chinese authorities to take action against malicious cyber activities undertaken from its territory; and Department of State (2020): The United States Condemns Russian Cyber Attack Against the Country of Georgia.
161 DFAT, Australian Government, ACSC, and Australian Government Department of Home Affairs (2020): UK-US-Canada Joint Advisory on Russia. References to international commitments will be further discussed in Section 3.6.
162 Auswärtiges Amt (2021): Cyberangriffe auf Bundestagsabgeordnete und Landtagsabgeordnete durch den Cyberakteur „Ghostwriter".
163 Auswärtiges Amt (2021): Cyberangriffe auf Bundestagsabgeordnete und Landtagsabgeordnete durch den Cyberakteur „Ghostwriter".
164 The White House (2021): The United States, Joined by Allies and Partners, Attributes Malicious Cyber Activity and Irresponsible State Behavior to the People's Republic of China.
165 Auswärtiges Amt (2021): Cyberangriffe auf Bundestagsabgeordnete und Landtagsabgeordnete durch den Cyberakteur „Ghostwriter".

States, delineated that it "consider[s] further steps to prevent, discourage, deter and respond to such malicious behaviour in cyberspace,"[166] while the U.S. included passages "reiterat[ing] that [...it would] take appropriate measures to defend [its] interests."[167] References like these can situate a specific OPPA within the broader response toolkit available to states and underline additional room for maneuver on the part of the attributing actor in addressing a particular threat.

Convergence among Focus Countries
Pointing out who is politically responsible constitutes a fundamental part of a state's attribution claim. Focus countries' OPPA practices showed similarity in that their OPPAs always specified who was being attributed. Regarding the provision of details on the perpetrator, focus countries' OPPAs demonstrated considerable variation, but specificity tended to increase over time, especially in OPPAs communicated via political channels. Regardless of the general differences that can be drawn between channels as general categories, the practices of focus countries also showed that specificity within channels were handled very differently by states. It would thus be premature to assess whether any or some of these levels represent a particular state's preferences. While there is agreement that some level should be included, convergence on what level of specificity to employ could not be traced. This low degree of convergence among focus countries' practices likewise extends to the provision of additional information on the attributed actor, which has not been provided comprehensively by states. Additionally, the second parameter covered in this finding—whether to include a message to the attributed actor—is one, if not the, parameter that offers itself the fewest of all for inclusion in any potential norm on responsible OPPA. This is because it will always likely be driven exclusively by sovereign national policy considerations on a case-by-case basis.

3.4 Only some OPPAs mention evidentiary information and estimative probability.

Evidence and technical analysis are essential for any attribution process and also impact a state's decision whether to go public with a given attribution. If they choose to go public, states may also decide to share some of the information underlying their attribution assessments. By publishing such evidence, attributing states can

166 Council of the European Union (2022): Russian cyber operations against Ukraine: Declaration by the High Representative on behalf of the European Union.
167 Department of State (2018): Joint Statement by Secretary of State Michael R. Pompeo and Secretary of Homeland Security Kirstjen Nielsen: Chinese Actors Compromise Global Managed Service Providers.

make claiming plausible deniability on the part of the attributed actors harder. This is of relevance, as, for example in the past, some of them have frequently raised the—according to them—"unsubstantiated"[168] nature of Western OPPAs directed at them. As UN Member States have agreed that they "should consider all relevant information"[169] when confronted with cybersecurity incidents, this parameter allows states to publicly display or provide indications as to what relevant information was considered, if they so wish. In doing so, focus countries may also seek to point out that their political attributions build upon a preceding technical attribution.

Moreover, at least conceptually, whether a state decides to shed light on evidence in its OPPA is also closely related to the inclusion of words of estimative probability (WEP) that can serve to "quantify the level of confidence [states] have in their evidence or their conclusions [...] via words or numbers,"[170] thereby reflecting "that attribution is gradual, not absolute."[171] From an external perspective, their inclusion can also facilitate comparability among various OPPAs.

In their OPPAs, the focus countries have acted on these two parameters in the following ways:

Table 5: Evidence & Estimative Probability—Options and Focus Countries' Practice

Parameter	Options	🇦🇺	🇩🇪	🇯🇵	🇺🇸
Provision of or reference to evidence	Mentioning of existence or general reliance on technical evidence without further details	○	●	●	●
	Reference to governmental sources of evidence	●	●	●	●
	Reference to commercial reporting	●	●	○	●
	Provision of technical information	●	●	●	●
Inclusion of estimative probability	Inclusion of a level of confidence or likelihood	○	●	●	●

168 Permanent Mission of the Russian Federation to the United Nations (2023): Statement by the Representative of the Russian Federation at the Fourth Session of the UN Open-Ended Working Group on Security of and in the Use of ICTs 2021-2025 and Iran (2023): Statement Mr. Heidar Ali Balouji First Counselor of the Permanent Mission of the Islamic Republic of Iran to the United Nations at the UNGA OEWG on ICTs.

169 UNGA (2015): Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (A/70/174).

170 Chris Cooley (2020): Words of Estimative Probability | A Threat Intelligence Reference.

171 Thomas Rid and Ben Buchanan (2014): Attributing Cyber Attacks, in: Journal of Strategic Studies 38 (1-2), pp. 4-37.

International consultation as a possible source of evidence alluded to within an OPPA will be discussed in the subsequent section (3.5).

Evidence

When comparing and evaluating the focus countries' practices in terms of the evidence their OPPAs provide, various trade-offs must be considered. Whether publishing evidence is desirable from the point of view of the attributing state greatly depends upon the communication channel chosen. This is because some, such as technical channels, may even necessitate some form of evidence, even if possibly provided out of different motivations. At the same time, not all types of channels are equally suited to accommodate various kinds of evidence, as, for example, "an indictment or press release does not lend itself to providing indicators of compromise [IOCs],"[172] which are often included in technical channels.

The extent of disclosure may also be subject to other factors, such as the target of the operation, as a state can be expected to provide less information when it itself has been the target of the operation, as opposed to the compromise of private sector actors. The scope of evidence provided also hinges on whether a cyber operation or campaign is attributed. In addition, the operation's severity and the question whether the operation is still ongoing can implicate the provision of evidence as more information may, for instance, be required for urgent mitigation purposes. The provision of evidence can also be aimed at the broader cybersecurity community and journalists as part of an effort to substantiate the attribution and, in turn, increase external support for a specific OPPA.

From an international stability point of view, there are reasons in favor of and against disclosing attribution evidence publicly.[173] On the one hand, referencing underlying evidence can increase the comprehensibility and credibility of the attribution assessment for other states. Similarly, this may permit insights into the decision-making process of a specific state, which can contribute to building confidence with third states. On the other hand, states may be reluctant to share evidence, as this

172 Kristen Eichensehr (2020): The Law & Politics of Cyberattack Attribution, in: UCLA Law Review 67, pp. 520-598. IOCs will be explained and discussed in the following.

173 It is worth noting that when it comes to the public attribution of an internationally wrongful act under international law, several states have indicated that they do not believe that there is an international legal requirement to give evidence to support attributions. Nonetheless, at least the positions of individual states appear to be shifting in this respect. For instance, the U.S. has noted in 2021 that it does not see an international legal obligation to reveal evidence on which attribution is based. But to facilitate global understanding of emerging state practice in this rapidly developing area, public attributions should, wherever feasible, include sufficient evidence to allow corroboration or cross-checking of allegations" (UNGA (2021): Official compendium of voluntary national contributions on the subject of how international law applies to the use of information and communications technologies by States submitted by participating governmental experts in the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security established pursuant to General Assembly resolution 73/266 (A /76/136)).

may reveal their sources and methods,[174] potentially compromising their intelligence operations and permitting adversaries to adapt their behaviors to evade attribution in the future. Including a reference to evidence in one OPPA may also impose some sort of self-obligation for further OPPAs to attribute only in similar situations of strong evidence.

Against this backdrop, focus countries have **referred to evidence without providing further details** in a few cases. For example, Germany once referred to unspecified reliable findings,[175] Japan highlighted that its OPPA was based on the "identifi[cation of] continuous attacks,"[176] or the U.S. denoted that it was "publicly attributing the massive WannaCry cyberattack [...] with evidence."[177] In other cases, the focus countries provided further insights into the origins of the evidence leading to their attributions. Such evidence originated either from their own government agencies or non-governmental entities.

Governmental Sources of Evidence

Among the governmental sources of evidence alluded to by focus countries were assessments provided by intelligence agencies of a state,[178] law enforcement investigations,[179] or insights gained from incident response activities by national cybersecurity agencies.[180] All four countries referenced findings from their security agencies in their alerts and advisories. In addition, almost all unsealed U.S. indictments and adopted sanctions included references to preceding law enforcement investigations. Contrary to other focus countries, which rarely mentioned the source of evidence in OPPAs communicated through political channels, Australia referred to "advice from Australian intelligence agencies" in a third of its public attribution statements.[181]

174 For instance, a joint advisory noted that it "contains the information we have concluded can be publicly released, consistent with the protection of sources and methods and the public interest" (FBI et al. (2023): Hunting Russian Intelligence "Snake" Malware).
175 Own translation, the OPPA noted "verlässliche Erkenntnisse" (Auswärtiges Amt (2021): Cyberangriffe auf Bundestagsabgeordnete und Landtagsabgeordnete durch den Cyberakteur „Ghostwriter").
176 Ministry of Foreign Affairs of Japan (2018): Cyberattacks by a group based in China known as APT10 (Statement by Press Secretary Takeshi Osuga).
177 The White House (2017): Press Briefing on the Attribution of the WannaCry Malware Attack to North Korea.
178 For example, Minister for Law Enforcement and Cyber Security (2018): Australian Government attribution of the 'NotPetya' cyber incident to Russia.
179 For example, National Police Agency (2021): 国家公安委員会委員長記者会見要旨.
180 For example, FBI and CISA (2022): Iranian Government-Sponsored APT Actors Compromise Federal Network, Deploy Crypto Miner, Credential Harvester.
181 For example, Minister for Law Enforcement and Cyber Security (2018): Australian Government attribution of cyber incident to Russia.

Commercial Sources of Evidence

Governmental attributions do not take place in a vacuum, as IT security companies also conduct and sometimes publish political attributions.[182] While a preceding private sector attribution may also increase pressure on the part of states and alter their decision calculus to react politically,[183] a cooperative relationship between governments and the private sector can increase or reinforce the former's technical attribution capabilities through additional threat intelligence input. States may thus also decide to reference private sector publications within their OPPAs.

In this respect, two focus countries—the U.S. and Germany—did so in some of their OPPAs. Australia has only been involved in one joint advisory with the U.S. that referenced private sector sources.[184] Given their shared emphasis on technical analysis, technical channels are particularly suited for pointing to private sector reporting. Germany has done so within its OPPAs through technical channels, whereas the U.S. has incorporated references to private sector attributions in all types of communication channels. Such references have taken various forms, including quotations within a technical channel's footnotes,[185] paraphrases of the findings of private sector reports,[186] or notes on the supplementary support of the attribution by "technical indicators from [...] the private sector."[187] In a few cases, the U.S. and Germany have also acknowledged contributions made by IT security companies.[188]

The possibility to touch upon private sector information can diminish both the pressure to disclose intelligence information and the need to entertain an intelligence gain/loss discussion. Simultaneously, referencing private sector attributions may also

182 On private sector attribution see also Sasha Romanosky and Benjamin Boudreaux (2020): Private-Sector Attribution of Cyber Incidents. Benefits and Risks to the U.S. Government, in: International Journal of Intelligence and CounterIntelligence 34 (3), pp. 463-493.

183 For instance, in her position piece, German Cyber Ambassador Grienberger, referred to high political pressure of naming the perpetrator that may be increased by the publication of information by a private company (Regine Grienberger (2023): Cyberangreifer benennen, globale Normen stärken: Erfahrungen mit dem Attributionsverfahren der Bundesregierung, Bundesakademie für Sicherheitspolitik). See also Kerstin Zettl-Schabath (2023): Staatliche Cyberkonflikte. Proxy-Strategien von Autokratien und Demokratien im Vergleich, transcript Verlag.

184 ACSC et al. (2022): Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure.

185 For example, ACSC et al. (2022): Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure.

186 For example, the German BfV once noted that an IT security company would have identified technical overlaps of the attributed activity with the Olympic Destroyer campaign that targeted the 2018 Winter Olympics in South Korea (BfV (2018): BfV Cyber-Brief Nr. 02/2018).

187 NCCIC and FBI (2016): GRIZZLY STEPPE – Russian Malicious Cyber Activity.

188 For example, the German BfV thanked a private sector company for the testing of detection rules and the provision of additional indicators (BfV (2019): BfV Cyber-Brief Nr. 01/2019) or the U.S. CISA noted that its advisory "provides information [...] obtained from FBI incident response activities and industry analysis of a Maui sample" (FBI, CISA and Department of the Treasury (2022): North Korean State-Sponsored Cyber Actors Use Maui Ransomware to Target the Healthcare and Public Health Sector). In one case, the U.S. mentioned private sector publications emphasizing that "industry reporting identifies three intrusion sets associated with the FSB, but the U.S. and UK governments have only formally attributed one of these sets—known as BERSERK BEAR—to FSB" (CISA (2022): Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure).

spare states from needing to make a direct attribution themselves. A recent example in this respect might represent the joint March 2023 advisory of German and South Korean authorities. Instead of directly naming North Korea as the attributed actor, the advisory used external reporting to avoid making a direct attribution itself. In a footnote on the specified attributed actor—KIMSUKY—it noted that "members of the IT security community regularly link KIMSUKY to North Korea's Reconnaissance General Bureau."[189] In this context, it is worth noting that the U.S. already attributed KIMSUKY to North Korea two and a half years prior.[190] This example underlines the political leeway, little as it may be, that states have in specifying the attributed actor within their OPPAs.

Provision of Technical Information

Especially in OPPAs disseminated via technical channels, but sometimes also political channels, Australia, Germany, Japan, and the U.S. provided technical information.[191] Technical information includes information on the vector of the operation, tactics, techniques, and procedures (TTPs)[192] of the attributed actor and IOCs[193] of the activity in question. It must be stressed that TTPs and IOCs do not themselves directly tie an operation or campaign to a state. Rather, they allow pinpointing an activity to a specific threat actor and give insights into its behavior. Linking this specific threat actor to another state requires taking into account other aspects, such as intelligence information and geopolitical analysis.[194] For instance, states stressed the exploitation of a specific vulnerability,[195] the deployment of

189 BfV (2023): Warning on KIMSUKY Cyber Actor's Recent Cyber Campaigns against Google's Browser and App Store Service.

190 CISA et al. (2020): North Korean Advanced Persistent Threat Focus: Kimsuky.

191 In addition to the evidence provided, technical OPPA channels usually always include a section on recommendations for mitigation of the activity attributed.

192 TTPs permit insights into "behaviors across the adversary lifecycle" (CISA (2021): Best Practices for MITRE ATT&CK® Mapping) to understand better what the attributed actor is doing as well as why and how it does so. Specifically, tactics represent the "adversary's technical goals, the reason for performing an action, and what they are trying to achieve", techniques reflect what actions the attributed actor has undertaken to achieve a particular goal, and procedures demonstrate "particular instances of how a technique [...] has been used" (CISA (2021): Best Practices for MITRE ATT&CK® Mapping).

193 "An indicator of compromise is a technical characteristic that—if found in system or network logs—is evidence for malicious activity [..., for] example [...] the IP address of a server used by an APT group" (Timo Steffens (2020): Attribution of Advanced Persistent Threats. How to Identify the Actors Behind Cyber-Espionage, Springer-Verlag). Inter alia, they can thus help organizations to detect whether they have been among the entities compromised by the operation attributed.

194 See further Timo Steffens (2020): Attribution of Advanced Persistent Threats. How to Identify the Actors Behind Cyber-Espionage, Springer-Verlag.

195 For example, NSA, CISA and FBI (2022): People's Republic of China State-Sponsored Cyber Actors Exploit Network Providers and Devices and Minister for Foreign Affairs, Minister for Home Affairs and Minister of Defence (2021): Australia joins international partners in attribution of malicious cyber activity to China.

(wiper) malware,[196] or distributed denial of service activities[197] by the attributed actor. They also noted tools and IT infrastructure used by the actor attributed, permitting them to shed light on, for example, how access was established or how communication with command-and-control servers was facilitated.[198]

As the provision of technical evidence in the form of TTPs and IOCs is usually reserved for technical channels, it is an interesting development that U.S. OPPAs in the form of political statements or indictments are increasingly being flanked by the simultaneous publication of a technical channel offering an additional level of insight informing the attribution decision.[199] Australia and Japan have each also issued a technical advisory/alert in addition to an OPPA statement by their respective Ministries of Foreign Affairs once. This may indicate an increased willingness on the part of these states to substantiate OPPAs in the form of political statements beyond pointing to the vector of the operation by referring to a corresponding technical channel for further evidence. However, this also requires a high degree of capacity on the part of the attributing state.

Estimative Probability

Alongside references to evidence, the U.S.,[200] Japan,[201] and Germany[202] have mentioned levels of confidence[203] or likelihood[204] with respect to their attribution assessments in minimal scope. Including such wording can signal to the attributed state a high attribution capacity and may demonstrate to other states and the

196 For example, Ministry of Foreign Affairs of Japan (2017): The U.S. Statement on North Korea's Cyberattacks (Statement by Press Secretary Norio Maruyama) and Department of State (2022): Attribution of Russia's Malicious Cyber Activity Against Ukraine.

197 For example, Minister for Foreign Affairs, Minister for Home Affairs and Minister of Defence (2022): Attribution to Russia for malicious cyber activity against European networks and Department of State (2022): Attribution of Russia's Malicious Cyber Activity Against Ukraine.

198 For example, BfV (2016): BfV Cyber-Brief Nr. 02/2016 and DHS and FBI (2017): HIDDEN COBRA – North Korea's DDoS Botnet Infrastructure.

199 For the first time in 2020 and in seven instances since, either a political or legal channel was simultaneously supported by a technical advisory (for example, in the Solar Winds and Microsoft Exchange exploitation cases). Zettl-Schabath describes this development under the Biden Administration as a triadic attribution approach comprising a political attribution in the form of an indictment, a joint domestic technical attribution in addition to a joint attribution statement with partner countries (see further Kerstin Zettl-Schabath (2023): Staatliche Cyberkonflikte. Proxy-Strategien von Autokratien und Demokratien im Vergleich, transcript Verlag).

200 For example, DHS, FBI, and National Cyber Security Centre (2018): Russian State-Sponsored Cyber Actors Targeting Network Infrastructure Devices.

201 Ministry of Foreign Affairs of Japan (2021): Cases of cyberattacks including those by a group known as APT40 which the Chinese government is behind (Statement by Press Secretary YOSHIDA Tomoyuki).

202 BMI (2016): Verfassungsschutzbericht 2015.

203 In its Guide to Cyber Attribution, the U.S. ODNI included the provision of a confidence level as a "best practice for presenting attribution analysis." In this framework, high confidence is assigned when the attribution determination has been made "beyond a reasonable doubt with no reasonable alternative," moderate confidence when the evidence is "clear and convincing, with only circumstantial cases for alternatives," and lastly low confidence in case "more than half of the body of evidence points to one thing, but there are significant information gaps" (ODNI (2018): A Guide to Cyber Attribution).

204 For instance, states may choose to quantify likelihood by mentioning words such as "certain", "almost certain", or "probable".

general public that the state in question exercises great care in pronouncing attribution assessments. Japan, in a statement, and the U.S., through both political and technical channels, have provided indications of confidence or likelihood with respect to the certainty with which the specific actor was argued to have conducted the operation attributed.[205] The U.S. also employed WEP to express the extent to which the attributed actor was considered to have used specific means to that end[206] and to articulate an estimate as to whether the operation attributed was still ongoing.[207] Germany used levels of likelihood to demonstrate the certainty with which it assessed a specific actor to operate as part of a particular state's intelligence services.[208] In its OPPAs, Australia did not explicitly use levels of confidence or likelihood and only employed verbs such as "confirm" or "assess" without further specification. Yet, former Australian Cyber Ambassador Feakin hinted that Australia would strive to reach a level of "beyond a reasonable doubt"[209] before proceeding with OPPAs.

Convergence among Focus Countries

Expectedly, the focus countries' OPPA practices did not allow to derive a requirement to include evidence in an OPPA, also given that it is a highly politicized matter. While there is little room for convergence among focus countries based on their practices, their attributions have nevertheless indicated that, despite their conceptual distinction, technical and political attribution are handled more fluidly in practice. Focus countries have considered technical channels as a particularly suitable option to share evidence. Given its low and not widespread rate of inclusion, as reflected in focus countries' practices, incorporating WEPs is one of the parameters that displayed the least amount of convergence in practice.

205 For example, The White House (2021): Fact Sheet: Imposing Costs for Harmful Foreign Activities by the Russian Government or The White House (2021): The United States, Joined by Allies and Partners, Attributes Malicious Cyber Activity and Irresponsible State Behavior to the People's Republic of China. Japan once used a level of likelihood to accentuate that it "assesses that it is highly likely that the Chinese government is behind APT40" (Ministry of Foreign Affairs of Japan (2021): Cases of cyberattacks including those by a group known as APT40 which the Chinese government is behind (Statement by Press Secretary YOSHIDA Tomoyuki)).

206 For example, CISA and FBI (2020): MAR-10295134-1.v1 – North Korean Remote Access Trojan: BLINDINGCAN.

207 For example, NSA, CISA, FBI and National Cyber Security Centre (2021): Russian GRU Conducting Global Brute Force Campaign to Compromise Enterprise and Cloud Environments.

208 BMI (2016): Verfassungsschutzbericht 2015.

209 Australian Foreign Affairs, Defence And Trade Legislation Committee (2019): Thursday, 24 October 2019, Official Committee Hansard.

3.5 States increasingly coordinate their OPPAs with like-minded countries.

In addition to domestic inter-agency OPPA practices, the international level and respective coordination with other states are playing an increasingly important role within the public attribution practices of the four focus countries.[210] In general terms, all focus countries highlighted the importance of international cooperation and a collective approach in responding to cyber operations, especially within political channels.[211] From the perspective of the attributing state, internationally coordinated public attributions are appealing because they can provide a broader information base, expand the legitimacy and impact of public attribution, and possibly decrease the risk of responsive repercussions on the part of the attributed actor against an individual state. The extent to which a public attribution can be internationally coordinated might also alter the decision calculus as to whether states are prepared to go public in the first place, as opposed to when they would have to shoulder potential consequences on their own.

At the same time, internationally coordinated attribution practices come with their own set of caveats. In this respect, timing may represent a challenge, as collaborative efforts ultimately require a balancing between the rapid ability to act on the one hand and the strive to get more states on board on the other hand. In addition, the international coordination of OPPAs is limited by the available capacities of the participating states, restricting, for example, the independent verification of intelligence information shared by other states to back up their attribution assertions. As the sharing of intelligence information often constitutes both a prerequisite and a challenge, international coordination on a specific OPPA is very likely limited to closely like-minded states. Beyond the particular operations in question, the extent of any international coordination on OPPA therefore rests highly upon trust and maintaining relationships between states.

Focus countries have engaged in international cooperation and coordination within their OPPAs in the following ways:

210 On international attribution mechanisms see also Isabella Brunner (2020): The Prospects for an International Attribution Mechanism for Cyber Operations – An Analysis of Existing Approaches.

211 Germany, for example, noted its determination to address cyber operations with European and international partners (Auswärtiges Amt (2022): Auswärtiges Amt verurteilt Cyberangriff der Russischen Föderation). In all its statements, Japan expressed its willingness to "continue to closely cooperate with the international community and make efforts in order to ensure a free, fair and secure cyberspace" (e.g. Ministry of Foreign Affairs of Japan (2021): Cases of cyberattacks including those by a group known as APT40 which the Chinese government is behind (Statement by Press Secretary YOSHIDA Tomoyuki)), one time also specifically mentioning the U.S. and G7 countries. Also Australia noted that it would be "working with allies and partners to improve cooperative global responses to malicious cyber activity that undermines international security and global economic stability" (Prime Minister and Minister for Foreign Affairs (2018): Attribution of a pattern of malicious cyber activity to Russia).

Table 6:
International Cooperation and Coordination—Options and Focus Countries' Practice

Parameter	Options	🇦🇺	🇩🇪	🇯🇵	🇺🇸
Engagement in international cooperation and coordination efforts	Participation in internationally coordinated attribution	●	●	○	●
	Support of OPPA practice by another state with own attribution assessment	●	○	●	●
	Support of OPPA practice by another state without own attribution assessment	●	●	●	○
	Retrospective endorsement of an OPPA by another state	○	●	○	○
	Reference to evidence of international origin or OPPAs of other states	●	●	●	●

Since the first OPPA in 2014,[212] all four focus countries have engaged in internationally coordinated OPPAs via political and technical channels. The first internationally coordinated OPPA by any focus country occurred in December 2017 by Australia, Japan, and the U.S. following the WannaCry ransomware operation.[213] Out of the 164 OPPAs analyzed, 25 cases had, to varying degrees, been internationally coordinated. A tabular overview outlining these 25 cases is contained in Annex V.

The attribution of responsibility for the Microsoft Exchange exploitations in July 2021 to Chinese actors constitutes the only time that all four focus countries (Germany via an EU statement) attributed the same operation. Three of the four focus countries were involved in the internationally coordinated OPPAs attributing the following cyber operations: WannaCry (2017), CloudHopper (2018), SolarWinds (2021, Germany via EU statement), and KA-SAT (2022). In 11 instances, two of the four focus countries attributed the same operation jointly or in very close temporal proximity.

International Coordination

When comparing these 25 instances, it becomes evident that international coordination has gradually increased. This also indicates that temporal constraints are decreasing, and the pace at which states can gain support from other states also willing and comfortable with going public is growing.

212 DOJ (2014): U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage.
213 Interestingly, this is in close temporal proximity to when the U.S. also started to use inter-agency coordinated public attribution, as highlighted in Section 3.1.

Focus countries have used three main types of international coordination with differing levels of coordination. Especially in the beginning of international coordination on OPPA, Australia, Japan, and the U.S. mainly used communication channels to support the OPPA by (an)other state(s) shortly after it had been issued. In the beginning, they did so regularly without, but subsequently often with an own supporting attribution assessment. In this respect, in the period investigated, Australia issued three supportive statements (in 2018,[214] 2020,[215] and 2021[216]), once with its own attribution confirmation (2021). All of Japan's attribution statements were phrased as a support to a preceding attribution practice of other countries—especially the U.S.—as theirs begin with a reference to the respective statements. The latest statements of 2018[217] and 2021[218] also included a reference to a national determination confirming the attribution to the respective attributed actor. The U.S. recently engaged in a public attribution supporting the attribution practices of multiple states by adding its own attribution assessment.[219] Germany (via an EU declaration issued in the name of the EU and its Member States) and a tweet by its Cyber Ambassador have twice supported the OPPA of another state without adding their own attribution assessment.[220] This also applies to a statement by the North Atlantic Council relating to the Microsoft Exchange operation, in which NATO Allies—including Germany—expressed their solidarity with the operation's victims and acknowledged that "Allies, such as Canada, the United Kingdom, and the United States, attribut[ed] responsibility for the Microsoft Exchange Server compromise to the People's Republic of China."[221] Prior to that, the international dimension of German public attribution practice was limited to a few cases that retrospectively endorsed previous OPPAs by other states,[222] requiring less to no international coordination, thus exemplarily illustrating enhanced international coordination in recent years.

214 Minister for Foreign Affairs (2018): Australia condemns the cyber operations attributed to Russia against the Organisation for the Prohibition of Chemical Weapons (OPCW) and against Malaysian locations participating in the Flight MH-17 investigation as revealed by Dutch and UK authorities overnight.

215 Department of Foreign Affairs, Australian Government, Australian Cyber Security Centre, and Australian Government Department of Home Affairs (2020): UK-US-Canada Joint Advisory on Russia.

216 Minister for Foreign Affairs, Minister for Home Affairs and Minister of Defence (2021): Attribution of cyber incident to Russia.

217 Ministry of Foreign Affairs of Japan (2018): Cyberattacks by a group based in China known as APT10 (Statement by Press Secretary Takeshi Osuga).

218 Ministry of Foreign Affairs of Japan (2021): Cases of cyberattacks including those by a group known as APT40 which the Chinese government is behind (Statement by Press Secretary YOSHIDA Tomoyuki).

219 Department of State (2022): Attribution of Russia's Malicious Cyber Activity Against Ukraine.

220 Council of the European Union (2021): Declaration by the High Representative on behalf of the European Union expressing solidarity with the United States on the impact of the SolarWinds cyber operation and GERonCyber (26.07.2022), X.

221 NATO (2021): Statement by the North Atlantic Council in solidarity with those affected by recent malicious cyber activities including the Microsoft Exchange Server compromise.

222 For instance, within its 2018 annual intelligence report of June 2019, the German domestic intelligence service highlighted that it would share the attribution assessment of UK and Dutch authorities as well as the UK and U.S., respectively for operations that occured in April and October 2018. It also once explicitly noted that this attribution confirmation would stem from its own findings.

Compared to the beginning, practices of support and endorsement have since been increasingly superseded by **joint public attributions**. Such internationally coordinated OPPAs have taken the form of joint technical advisories or jointly coordinated political statements. All focus countries, except for Japan, have engaged in such practices. In contrast to expressions of support, as previously discussed, OPPAs matching this type of international coordination refer to a joint and simultaneous attribution effort—in contrast to support statements phrased as building upon a preceding attribution by (an)other state(s). When it comes to internationally coordinated political statements, it is noteworthy that compared to Australia,[223] the U.S.[224] rarely explicitly mentioned that their OPPA were being communicated following engagement and consultation with other states. Notwithstanding, the U.S. actively appealed to other states in its OPPAs to "join [the U.S.] in holding malicious cyber actors accountable"[225] to prospectively expand the circle of countries engaged in OPPA efforts. Compared to the U.S. and Australia, Germany's joint international attribution practice remains limited. Its primary vehicle to this end did not represent ad hoc coordinated like-minded coalitions, seemingly the U.S. and Australian preference, but public attribution within the framework of the EU.[226]

223 In seven out of 12 cases, Australian statements alluded that Australia would join other states, four times by mentioning specific countries, such as the U.S., UK, and the EU, or three times by making a more general reference to partners, in arriving and publicly highlighting the respective attributions. On the coordinated July 2021 Microsoft Exchange, a representative of the Australian Department of Home Affairs shared a few days later in the Australian Parliament that the U.S. would have consulted Australia before. He also went on record highlighting that "given the way in which the attribution action occurred across the world, it was obviously synchronized and coordinated" (Australian Parliamentary Joint Committee on Intelligence and Security (2021): Thursday, 29 July 2021, Official Committee Hansard). A few months earlier in March 2021, Australian Cyber Ambassador Feakin shared that Australia would "often get requests from allied partners or share those with others to build joint attributions together" (Australian Foreign Affairs, Defence And Trade Legislation Committee (2021): Thursday, 25 March 2021, Official Committee Hansard).

224 The U.S. only explicitly mentioned international engagement on the respective OPPAs three times: in the case of WannaCry in December 2017, following the Microsoft Exchange exploitation in July 2021, and a February 2022 press briefing highlighting Russian operations against Ukrainian banks. All of these three OPPAs have in common that they were issued at the White House-level. Other U.S. OPPA's which very likely have entailed an active international coordination on the part of the U.S. given respective OPPAs by other like-minded countries in close temporal proximity are (in chronological order): NotPetya, WADA, OPCW, CloudHopper, Georgia, SolarWinds, and Ukraine II (see further Annex V).

225 The White House (2022): Statement by NSC Spokesperson Adrienne Watson on Iran's Cyberattack against Albania. See also Department of State (2020): United States Charges Russian Military Intelligence Officers for Cyber Crimes or Department of State (2021): Responding to the PRC's Destabilizing and Irresponsible Behavior in Cyberspace.

226 Publicly, Germany noted that—as of April 2022—results of its national attribution process contributed to the EU declarations on SolarWinds (which exclusively refers to the U.S. attribution and does not attribute on its own), Microsoft Exchange and Ghostwriter (Auswärtiges Amt (2022): Jahresabrüstungsbericht 2021). The EU declaration on Ghostwriter was preceded by a German national statement. Subsequently, Germany raised the issue at the EU level and initiated respective consideration of the operation within the framework of the EU.

OPPA at the EU Level

As part of the so-called EU Cyber Diplomacy Toolbox established in 2017,[227] EU Member States agreed in 2019 on guidelines for "coordinated attribution at EU level,"[228] acknowledging that attribution remains a national prerogative. One or multiple EU Member States can initiate the process toward a coordinated attribution. The decision on whether to coordinate and/or to publish a coordinated attribution rests with the Council of the EU, composed of representatives of all EU Member States, thus requiring consensus among all 27 Member States. When a decision is made, the Council may also consider facilitating a coordinated attribution with other non-EU countries or regional/international organizations. It is important to note that sanctions possibly agreed upon within the framework of the EU Cyber Diplomacy Toolbox do not require a political attribution and are deliberately not considered as such, also since they can only be directed at legal or natural persons.[229]

As for statements, joint advisories constitute a more recent practice for Germany, with the first, and so far only, joint advisory including an attribution issued in March 2023 with South Korean authorities.[230] Compared to Germany, especially the U.S., but also the Australian practice of joint international advisories has evolved significantly since 2018. Given the close relationship between their agencies in the framework of the Five Eyes intelligence alliance, it is unsurprising that particularly agencies from the United Kingdom, Canada, and sometimes New Zealand take part in coordinated attribution.[231]

227 Council of the European Union (2017): Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities („Cyber Diplomacy Toolbox"), 19 June 2017 and Council of the European Union (2017): Draft implementing guidelines for the Framework on a Joint EU Diplomatic Response to Malicious Cyber Activities - approval of the final text.

228 European External Action Service (n.d.): Framework for a joint EU diplomatic response to malicious cyber activities "cyber diplomacy toolbox". The guidelines are not public, an earlier draft of the guidelines giving a good overview of its foreseen scope and key points can be found here: Council of the European Union (2019): Implementation of the Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities - Attribution of malicious cyber activities - discussion of a revised text.

229 Council of the European Union (2019): Council Decision (CFSP) 2019/797 of 17 May 2019 concerning restrictive measures against cyber-attacks threatening the Union or its Member States. On EU cyber sanctions, see also Julia Grauvogel and Christian von Soest (2021): Cybersanktionen: Zunehmende Anwendung eines neuen Instruments.

230 The advisory was issued together with the South Korean National Intelligence Service and attributed activity to threat actor KIMSUKY (BfV (2023): Warning on KIMSUKY Cyber Actor's Recent Cyber Campaigns against Google's Browser and App Store Service).

231 From the OPPAs analyzed, the U.S. has participated in joint international advisories in nine instances and Australia participated in three of them. In all joint advisories that Australia took part in, U.S. and UK authorities were among the authoring agencies. Canadian and New Zealandian entities were involved three and two times respectively. The U.S. has also ventured once beyond the Five Eye countries and published a joint advisory in February 2023 with South Korea.

International Cooperation

In addition to coordinating individual OPPAs, states also referred to international cooperation within their public attributions with respect to evidence and information-sharing. Australia and the U.S. pointed to consultations with other states or the provision of foreign information as a (supplementary) basis for attribution assessments.[232] For instance, in two-thirds of its statements, Australia noted that its attribution assessments were made "in consultation with our partners."[233] In contrast, the U.S. tended to indicate in its OPPAs made via political channels, that it shared respective information with other states. For example, it noted that like-minded countries "have seen [their] analysis"[234] or highlighted that it had "shared the underlying intelligence"[235] with other states.

When it comes to criminal law channels, the respective press releases frequently noted international cooperation during investigations that led to the particular indictments, for instance, by naming the contribution of specific partner authorities.[236] Less explicit than these examples, Japan referenced a U.S. CISA advisory in its latest alert, also emphasizing that it drew on the respective information as part of its attribution assessment.[237] While some degree of international information-sharing can be assumed to occur preceding many, if not most, attributions, highlighting it within OPPAs may also increase reliability by permitting cross-validation. It can also serve as a safeguard in the sense that it may decrease the potential for responses on the part of the attributed government to be directed at only one state.

232 Neither Germany nor Japan have explicitly referred to foreign evidence informing its attribution deliberations within specific OPPAs. However, for example, German Cyber Ambassador Grienberger has shared that information from partners would be essential for an appropriate evaluation (Regine Grienberger (2023): Cyberangreifer benennen, globale Normen stärken: Erfahrungen mit dem Attributionsverfahren der Bundesregierung, Bundesakademie für Sicherheitspolitik). Also, in the case of Japan, there have been subsequent indications by an anonymous government official cited in the press that the Japanese statement on the WannaCry operation would have been informed by classified U.S. intelligence (Nikkei (2021): JAXAサイバー攻撃に反撃　日本初「特定」の狙い).

233 For example, Minister for Foreign Affairs, Minister for Home Affairs and Minister of Defence (2021): Australia joins international partners in attribution of malicious cyber activity to China.

234 The White House (2017): Press Briefing on the Attribution of the WannaCry Malware Attack to North Korea.

235 The White House (2022): Press Briefing by Press Secretary Jen Psaki, Deputy National Security Advisor for Cyber and Emerging Technology Anne Neuberger, and Deputy National Security Advisor for International Economics and Deputy NEC Director Daleep Singh, February 18, 2022.

236 For example, DOJ (2018): Nine Iranians Charged With Conducting Massive Cyber Theft Campaign on Behalf of the Islamic Revolutionary Guard Corps and DOJ (2020): Six Russian GRU Officers Charged in Connection with Worldwide Deployment of Destructive Malware and Other Disruptive Actions in Cyberspace.

237 National Police Agency, Financial Services Agency & National Center of Incident Readiness and Strategy for Cybersecurity (2022): 北朝鮮当局の下部組織とされるラザルスと呼称されるサイバー攻撃グループによる暗号資産関連事業者等を標的としたサイバー攻撃について（注意喚起）.

Convergence among Focus Countries
Focus countries' practice indicated that international coordination on OPPAs is increasing. Especially when it comes to political channels, some degree of international coordination did even—seemingly—represent a prerequisite for some states to engage in OPPA, as, for example, both Australia and Japan never issued a unilateral, not internationally coordinated OPPA when using a political channel (Australia also in its use of technical channels). Similarly, since establishing its attribution process, Germany also exclusively engaged in multilateral OPPAs. There thus appears to be some consensus among focus countries that, if possible, states should at least consult like-minded states before publicizing their OPPAs. However, whether such consultations extend to the actual pursuit of an internationally coordinated OPPA in individual instances cannot be pre-determined and remains a national decision on a case-by-case basis.

3.6 States regularly explain why they attribute, pointing to the operation, their policies, past OPPAs, and/or international commitments.

The parameters touched upon in sections 3.1-3.5 have focused on both what has been attributed and how the focus countries have conducted their OPPAs. However, they leave open the question of why states publicly attributed the respective operations in the first place. Often, focus countries have included or at least given a glimpse into their reasoning within their OPPA practices, primarily when political channels were used.

In explaining why they did so, the focus countries pointed to different reasons as follows:

Table 7: Reasons for Pursuing OPPAs—Options and Focus Countries' Practice

Parameter	Options	🇦🇺	🇩🇪	🇯🇵	🇺🇸
Specification of the severity of the operation attributed	Indication of effect and/or impact of operation attributed	●	●	○	●
	Indication of threats and/or risks posed by operation attributed	●	●	●	●
	Indication of assumed goals of attributed actor	●	●	○	●
Formulation of policy objectives pursued with OPPA	Exposure of or response to malicious cyber activity	●	●	●	●
	Imposition of pressure, costs, or consequences	●	○	●	●
	Provision of information, awareness raising, and/or warning of organizations	●	●	●	●
	Defense and protection of national interests or allies	○	○	○	●
Linkage to national (attribution) policy	Reference to national strategies/policy documents	●	○	○	●
	Mentioning of domestic or international cybersecurity response actions	●	○	○	●
Inclusion of reference to prior OPPAs	Inclusion of a reference to own previous OPPA practices in general or to the same attributed actor	●	○	●	●
Reference to cyber norms or other commitments	Indirect or explicit reference to UN cyber norms or the framework of responsible state behavior	●	●*	●	●
	Reference to bilateral or international commitments	●	○	●	●
	Mentioning non-compliance with a specific cyber norm or other commitments	○	○	○	●

While each reason represents a distinct parameter, they are considered together in this section because they can be mutually reinforcing when employed. Stating all or some of these reasons may offer states a way to influence the OPPA's narrative

and framing for its audience. Insights into a state's reasoning can increase the perceived policy coherence, the predictability of how policies are enacted, and the comprehensibility of a country's attribution decision. The extent to which states act on these parameters also highly depends on whether foreign or domestic policy motivations are pursued and which type of channel is being used. Regarding the latter, the focus countries have especially included reasons when they communicated OPPAs via political channels.

Severity of Operation Attributed

When it comes to clarifying the reasons why the operation in question was attributed, the focus countries have indicated various aspects, including specifying its effect and impact, the threat and risks it poses, and details on the assumed goals of the attributed actor, building upon the factual description of the operation attributed. This parameter allows states to emphasize particular elements of the operation that they deem particularly concerning, which can provide a narrative as to why the OPPA has been pursued or deepen it. What information states include may also permit insights into what factors play a role in determining whether to pursue public attribution in general.[238] In this respect, specifications of the operation's severity can also contribute to shaping common understandings about what kind of behavior states do not tolerate. Relevant to the evidence parameter discussed in section 3.4, the more details are provided in this respect, the more the need arises to also substantiate these claims or provide some background.

Effect and Impact

Relating to the effect and impact of the operation, Australia and the U.S. have, for example, expressed that the operation attributed was "disruptive"[239] (Georgia) and/or "destructive"[240] (Viasat). Both states also indicated whether the operations of (critical) infrastructure providing services to the public had been suspended

238 The United Kingdom, for example, has publicly communicated that its decision whether or not to engage in OPPA is guided by the following aspects: geopolitical and bilateral factors, impact on victim, impact on law enforcement activity, UK values and ability to operate, as well as wider response options. Details can be found here: Foreign and Commonwealth Office (2019): Non-Paper on Efforts to Implement Norms of Responsible State Behaviour in Cyberspace, as Agreed in UN Group of Government Expert Reports of 2010, 2013 and 2015.

239 For example, Minister for Foreign Affairs (2020): Attribution of malicious cyber activity in Georgia to Russian Military Intelligence.

240 For example, Department of State (2022): Attribution of Russia's Malicious Cyber Activity Against Ukraine.

or interrupted.[241] In addition, in some instances, the U.S. mentioned that systems had been rendered "inoperable"[242] or "useless."[243] Australia,[244] Germany,[245] and the EU[246] mentioned spill-over effects caused by the operation to entities located in countries other than the intended target that affected uninvolved third parties. The U.S., Germany, and the EU also specified whether data has been compromised or stolen.[247] In a few cases, Australia and the U.S. added whether this includes data of a confidential or sensitive nature.[248] In some of their OPPAs, Australia, Germany, and the U.S. included details on the sophistication of either the operation or the methods used by the attributed actor. For example, Australia, Germany, and the U.S. outlined the sophistication of tools used by the attributed actor,[249] the U.S. laid out if the attributed operation was "unprecedented,"[250] or Germany mentioned whether the attributed actor was considered to have used a significant amount of resources to conduct the attributed operation.[251]

Threats and Risks

Different from effect and impact, outlining threats and/or risks posed by the operation attributed offers states the opportunity to highlight what they consider implicated and worth protecting. In this respect, all focus countries sometimes highlighted to varying degrees that the operations attributed represented a threat

241 For example, the U.S. indicated that "cyber threat actors [...] disrupted Albanian government computer systems, forcing the government to suspend online public services for its citizens" (Department of the Treasury (2022): Treasury Sanctions Iranian Ministry of Intelligence and Minister for Malign Cyber Activities) and in its attribution of the NotPetya operation, Australia highlighted that the operation had "interrupted the normal operation of banking, power, airports and metro services in Ukraine" (Minister for Law Enforcement and Cyber Security (2018): Australian Government attribution of the 'NotPetya' cyber incident to Russia).

242 For example, FBI (2014): Update on Sony Investigation.

243 For example, The White House (2017): Press Briefing on the Attribution of the WannaCry Malware Attack to North Korea.

244 Minister for Foreign Affairs, Minister for Home Affairs and Minister of Defence (2022): Attribution to Russia for malicious cyber activity against European networks.

245 Auswärtiges Amt (2022): Auswärtiges Amt verurteilt Cyberangriff der Russischen Föderation.

246 Council of the European Union (2021): China: Declaration by the High Representative on behalf of the European Union urging Chinese authorities to take action against malicious cyber activities undertaken from its territory.

247 Department of State (2022): Attribution of Russia's Malicious Cyber Activity Against Ukraine; DOJ (2018): Two Chinese Hackers Associated With the Ministry of State Security Charged with Global Computer Intrusion Campaigns Targeting Intellectual Property and Confidential Business Information; BMI (2019): Verfassungsschutzbericht 2018; and Council of the European Union (2021): Declaration by the High Representative on behalf of the European Union on respect for the EU's democratic processes.

248 For example, DOJ (2020): Chinese Military Personnel Charged with Computer Fraud, Economic Espionage and Wire Fraud for Hacking into Credit Reporting Agency Equifax; DOJ (2018): Two Chinese Hackers Associated With the Ministry of State Security Charged with Global Computer Intrusion Campaigns Targeting Intellectual Property and Confidential Business Information; and Prime Minister and Minister for Foreign Affairs (2018): Attribution of a pattern of malicious cyber activity to Russia.

249 FBI et al. (2023): Hunting Russian Intelligence "Snake" Malware and BfV (2016): BfV Cyber-Brief Nr. 02/2016.

250 The White House (2022): Statement by NSC Spokesperson Adrienne Watson on Iran's Cyberattack against Albania.

251 BfV (2016): BfV Cyber-Brief Nr. 02/2016. In this alert, the German BfV also noted that the operation would be "in Umfang und Qualität herausragend" [outstanding in scope and quality, own translation].

or risk to their own national security.[252] The U.S. and Australia have additionally accentuated national security concerns of an allied or partner state.[253] In this respect, Australia also alluded to international stability and security more broadly, as well as its "government operations"[254] as potentially impacted areas of significance requiring protection.[255] Moreover, Japan,[256] Germany,[257] the EU,[258] Australia,[259] and the U.S. underlined threats or risks to democratic decision-making processes, for example, "to undermine the democratic processes and institutions essential to the functioning of our democracy and that of other countries."[260] The U.S.,[261] Australia,[262] and the EU[263] mentioned implications for the (global) economy and the integrity of the (international) financial system. Additionally, the U.S. and Australia invoked "public safety"[264] or the "safety and welfare of individuals,"[265] whereas Japan frequently alluded to the "security of cyberspace"[266] that is or can be impacted by the attributed behavior.

252 For example, Minister for Foreign Affairs, Minister for Home Affairs and Minister of Defence (2021): Australia joins international partners in attribution of malicious cyber activity to China; Auswärtiges Amt (2021): Cyberangriffe auf Bundestagsabgeordnete und Landtagsabgeordnete durch den Cyberakteur „Ghostwriter"; Council of the European Union (2021): China: Declaration by the High Representative on behalf of the European Union urging Chinese authorities to take action against malicious cyber activities undertaken from its territory; and Ministry of Foreign Affairs of Japan (2021): Cases of cyberattacks including those by a group known as APT40 which the Chinese government is behind (Statement by Press Secretary YOSHIDA Tomoyuki).

253 For example, Minister for Foreign Affairs, Minister for Home Affairs and Minister of Defence (2022): Attribution to Russia of malicious cyber activity against Ukraine and The White House (2022): Statement by NSC Spokesperson Adrienne Watson on Iran's Cyberattack against Albania.

254 For example, Minister for Law Enforcement and Cyber Security (2018): Australian Government attribution of the 'NotPetya' cyber incident to Russia.

255 Minister for Foreign Affairs, Minister for Home Affairs and Minister of Defence (2021): Australia joins international partners in attribution of malicious cyber activity to China and Prime Minister and Minister for Foreign Affairs (2018): Attribution of a pattern of malicious cyber activity to Russia.

256 Ministry of Foreign Affairs of Japan (2021): Cases of cyberattacks including those by a group known as APT40 which the Chinese government is behind (Statement by Press Secretary YOSHIDA Tomoyuki).

257 Auswärtiges Amt (2022): Auswärtiges Amt verurteilt Cyberangriff der Russischen Föderation.

258 Council of the European Union (2021): Declaration by the High Representative on behalf of the European Union on respect for the EU's democratic processes.

259 Minister for Foreign Affairs (2020): Attribution of malicious cyber activity in Georgia to Russian Military Intelligence.

260 Department of State (2022): Targeting Russia's Global Malign Influence Operations and Election Interference Activities.

261 For example, CISA et al. (2020): FASTCash 2.0: North Korea's BeagleBoyz Robbing Banks.

262 For example, Minister for Law Enforcement and Cyber Security (2018): Australian Government attribution of the 'NotPetya' cyber incident to Russia.

263 For example, Council of the European Union (2021): China: Declaration by the High Representative on behalf of the European Union urging Chinese authorities to take action against malicious cyber activities undertaken from its territory.

264 The White House (2021): Fact Sheet: Imposing Costs for Harmful Foreign Activities by the Russian Government. Australia has referred to public safety in the following OPPA: Minister for Foreign Affairs, Minister for Home Affairs and Minister of Defence (2021): Attribution of cyber incident to Russia.

265 Minister for Law Enforcement and Cyber Security (2018): Australian Government attribution of the 'NotPetya' cyber incident to Russia. In a similar vein, in one of its OPPAs the U.S. mentioned that the operation in question "pose[d] an elevated risk of harm to the population" (The White House (2022): Statement by NSC Spokesperson Adrienne Watson on Iran's Cyberattack against Albania).

266 For example, Ministry of Foreign Affairs of Japan (2021): Cases of cyberattacks including those by a group known as APT40 which the Chinese government is behind (Statement by Press Secretary YOSHIDA Tomoyuki).

Assumed Goals of Attributed Actor

Within their reasoning, the U.S., Australia[267], and Germany[268] also recounted the assumed goals and gains of the attributed actor. The inclusion of corresponding assumptions permits states to embed the operation or campaign attributed in the broader policy goals of the attributed actor, which can underline the perceived necessity of resorting to an OPPA. For example, in one of its OPPAs, the U.S. stressed that Iranian APT groups were "likely intent on influencing and interfering with the U.S. elections to sow discord among voters and undermine public confidence in the U.S. electoral process."[269] The U.S. also pointed out the advancement of national security objectives,[270] the exercise of influence on foreign policies,[271] the circumvention of sanctions,[272] the facilitation of a competitive advantage,[273] or the silencing of journalists or dissidents[274] that the attributed actor might have sought or derived from the operation attributed. States also underscored whether the intended or impacted targets were of reconnaissance, economic, political, or other strategic interest or relevance to the attributed actor.[275]

In shedding light on the attributed actor's goals, Germany and the U.S. also outlined whether the operation stood individually or was part of a broader multi-stage intrusion, for example, in preparation for subsequent influence operations[276] or to "disrupt and damage [...] at a future time of [the attributed actor's] choosing."[277] In a similar vein, in a few instances, the U.S., Germany, and Australia highlighted how the operation attributed relates to other activities by the attributed actor (not

267 Minister for Foreign Affairs, Minister for Home Affairs and Minister of Defence (2022): Attribution to Russia for malicious cyber activity against European networks.
268 BMI (2015): Verfassungsschutzbericht 2014.
269 CISA and FBI (2020): Iranian Advanced Persistent Threat Actors Threaten Election-Related Systems.
270 For example, DHS, FBI and National Cyber Security Centre (2018): Russian State-Sponsored Cyber Actors Targeting Network Infrastructure Devices.
271 For example, FBI and CISA (2020): Russian State-Sponsored Advanced Persistent Threat Actor Compromises U.S. Government Targets.
272 For example, FBI, CISA, and Department of Treasury (2021): AppleJeus: Analysis of North Korea's Cryptocurrency Malware.
273 For example, DOJ (2014): U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage.
274 For example, Department of State (2020): The United States Sanctions Cyber Actors Backed by Iranian Intelligence Ministry and BfV (2023): Warning on KIMSUKY Cyber Actor's Recent Cyber Campaigns against Google's Browser and App Store Service.
275 For example, the U.S. has outlined that "some victim accounts were of predictable interest to the FSB" (DOJ (2017): U.S. Charges Russian FSB Officers and Their Criminal Conspirators for Hacking Yahoo and Millions of Email Accounts) or Germany has mentioned that the "Zielauswahl zeigt ein staatliches Aufklärungsinteresse" [target selection displays a governmental reconnaissance interest, own translation] (Bundesamt für Verfassungsschutz (2016): BfV Cyber-Brief Nr. 02/2016).
276 Own translation, the press conference spoke of "Vorbereitungshandlungen für Einflussoperationen" (Auswärtiges Amt (2021): Cyberangriffe auf Bundestagsabgeordnete und Landtagsabgeordnete durch den Cyberakteur „Ghostwriter").
277 DOJ (2022): Four Russian Government Employees Charged in Two Historical Hacking Campaigns Targeting Critical Infrastructure Worldwide.

necessarily exclusively regarding cyber operations)[278] or linked it to previously identified behavioral patterns of the attributed actor.[279] Especially in recent years, states emphasized that there was a political or temporal context of relevance to the operations attributed.[280] For example, in February 2022, the U.S. noted that the "recent spate of cyberattacks in Ukraine [...could lay] the groundwork for more disruptive cyberattacks accompanying a potential further invasion of Ukraine's sovereign territory."[281]

Policy Objectives

In addition to shedding light on the operation in question, states may also provide explanations as to why they are pursuing an OPPA in a specific case through the formulation of policy objectives. All states (Germany via the EU), particularly Australia and the U.S., have expressed their motivation to **expose or respond to malicious cyber activity**.[282] In a similar vein, all focus countries except Germany pointed out their desire to **impose costs, consequences, or pressure** on the attributed actor through the OPPA.[283] The U.S. also sought to impose costs to make the attributed actor change or cease its behavior[284] and in an effort to "hold [it]

278 For example, Auswärtiges Amt (2021): Cyberangriffe auf Bundestagsabgeordnete und Landtagsabgeordnete durch den Cyberakteur „Ghostwriter" and Department of State (2020): The United States Condemns Attempts by P.R.C.-Affiliated Actors To Steal American COVID-19 Research.

279 For example, Minister for Foreign Affairs (2020): Attribution of malicious cyber activity in Georgia to Russian Military Intelligence.

280 For example, Auswärtiges Amt (2022): Auswärtiges Amt verurteilt Cyberangriff der Russischen Föderation; Bundesministerium des Innern (2015): Verfassungsschutzbericht 2014.

281 The White House (2022): Press Briefing by Press Secretary Jen Psaki, Deputy National Security Advisor for Cyber and Emerging Technology Anne Neuberger, and Deputy National Security Advisor for International Economics and Deputy NEC Director Daleep Singh, February 18, 2022.

282 For example, Minister for Foreign Affairs, Minister for Home Affairs and Minister of Defence (2022): Attribution to Russia of malicious cyber activity against Ukraine; Minister for Foreign Affairs, Minister for Home Affairs and Minister of Defence (2021): Australia joins international partners in attribution of malicious cyber activity to China; Council of the European Union (2021): China: Declaration by the High Representative on behalf of the European Union urging Chinese authorities to take action against malicious cyber activities undertaken from its territory; Ministry of Foreign Affairs of Japan (2021): Cases of cyberattacks including those by a group known as APT40 which the Chinese government is behind (Statement by Press Secretary YOSHIDA Tomoyuki); The White House (2021): The United States, Joined by Allies and Partners, Attributes Malicious Cyber Activity and Irresponsible State Behavior to the People's Republic of China; and Department of State (2020): United States Sanctions Russian Government Research Institution.

283 For example, Japan alluded that its attribution would be guided "from the perspective of maximizing pressure on North Korea to alter its policy" (Ministry of Foreign Affairs of Japan (2017): The U.S. Statement on North Korea's Cyberattacks (Statement by Press Secretary Norio Maruyama)) or Australia referenced the need to "impos[e] costs on state-based or state-sponsored malicious actors who seek to undermine an open, free, safe and secure cyberspace" (Minister for Foreign Affairs, Minister for Home Affairs and Minister of Defence (2022): Attribution to Russia for malicious cyber activity against European networks).

284 For example, U.S. OPPA practices laid out that "some of the benefit that comes from this attribution is letting them know that we're going to move to stop their behavior" (The White House (2017): Press Briefing on the Attribution of the WannaCry Malware Attack to North Korea) or noted that "by calling out the individuals and nations who use cyber attacks to threaten American enterprise, as we have done in this indictment, we will change behavior" (DOJ (2016): Seven Iranians Working for Islamic Revolutionary Guard Corps-Affiliated Entities Charged for Conducting Coordinated Campaign of Cyber Attacks Against U.S. Financial Sector).

accountable."[285] Unlike other focus countries, the U.S. also invoked the **defense and protection of national interests and allies**[286] as driving factors behind its decision to move for an OPPA. These three policy objectives have been particularly alluded to within OPPAs through political channels. In contrast, the focus countries' practices within technical channels—but also statements to a lesser degree—emphasized the objective of **providing information, raising awareness, and/or warning organizations**, catering predominantly to a domestic audience.[287] For instance, Germany stated that one of its alerts including an OPPA was published in an effort to draw the attention of German companies to the exposed threat situation,[288] or that it had published an advisory to "raise awareness of KIMSUKY's [...] cyber campaigns [...] targeting experts on the Korean Peninsula and North Korea issues."[289]

National (Attribution) Policy

Aside from mentioning individual policy objectives driving the decision to publish an OPPA, governments have also linked OPPAs to their national (attribution) policies. As for the formulation of policy objectives, such linkage can serve to reflect domestic policy considerations and priorities. Across cases, Australia and the U.S. linked their OPPAs to their national (attribution) policies particularly often. They did so in various ways, such as **referencing policy documents, like national or international cybersecurity strategies**. For example, Australia underscored that its "2017 International Cyber Engagement Strategy commits Australia to deter and respond to malevolent behaviour in cyberspace,"[290] or the U.S. brought up that "accountability and cooperation are the cornerstone principles of [its] cybersecurity strategy."[291] Australia and the U.S. also highlighted specific **domestic or international cybersecurity response actions** within their OPPAs. For example, the U.S. pointed out efforts to "modernize federal networks and improve

285 DOJ (2021): Four Chinese Nationals Working with the Ministry of State Security Charged with Global Computer Intrusion Campaign Targeting Intellectual Property and Confidential Business Information, Including Infectious Disease Research.

286 For example, Department of State (2018): Joint Statement by Secretary of State Michael R. Pompeo and Secretary of Homeland Security Kirstjen Nielsen: Chinese Actors Compromise Global Managed Service Providers and Department of State (2020): The United States Sanctions Cyber Actors Backed by Iranian Intelligence Ministry.

287 For example, a White House Statement concluded by noting that the OPPA would also represent a means to "inform and empower system owners and operators to act" (The White House (2021): The United States, Joined by Allies and Partners, Attributes Malicious Cyber Activity and Irresponsible State Behavior to the People's Republic of China) or Australia called upon "governments, the private sector and households [to] remain vigilant about the ongoing threats we face in cyberspace" (Minister for Foreign Affairs, Minister for Home Affairs and Minister of Defence (2022): Attribution to Russia of malicious cyber activity against Ukraine). Japan has once issued a simultaneous alert to a statement "to call upon adequate domestic cybersecurity measures" (Ministry of Foreign Affairs of Japan (2018): Cyberattacks by a group based in China known as APT10 (Statement by Press Secretary Takeshi Osuga)).

288 BfV (2017): BfV Cyber-Brief Nr. 02/2017.

289 BfV (2023): Warning on KIMSUKY Cyber Actor's Recent Cyber Campaigns against Google's Browser and App Store Service.

290 Minister for Law Enforcement and Cyber Security (2018): Australian Government attribution of cyber incident to Russia.

291 The White House (2017): Press Briefing on the Attribution of the WannaCry Malware Attack to North Korea.

the nation's cybersecurity, including of critical infrastructure"[292] and announced specific follow-up measures to impacted entities such as "offer[ing] additional capacity building and technical assistance to help strengthen Georgia's public institutions and improve its ability to protect itself from these kinds of activities."[293] When included, Australian OPPA practices particularly emphasized domestic actions taken, encompassing, for example, financial investments to increase capacity and new legislative proposals or strategies.[294] Partly, Australia also mentioned activities involving other countries, such as the provision of assistance and training or the initiation of a bilateral dialogue on cybersecurity policy.[295]

Prior OPPAs

Australia, Japan, and the U.S. also included **references to either their own previous OPPA practices in general or, if applicable, to the same attributed actor**. They may have done so to establish coherence between different OPPA practices and to provide a comprehensive public record of the attributed actor's activities. For example, in one of its three statements, Japan referred to a prior attribution of another operation to China.[296] Australia included references to the year it first engaged in an OPPA and shed light on recent examples of previous attributions to other actors and the same attributed country.[297] U.S. OPPA practices predominantly included references to prior attributions to the same actor.[298] At times, U.S. technical channels have also been updated in retrospect to include a U.S. government attribution of previously highlighted malicious activities.[299]

292 The White House (2021): The United States, Joined by Allies and Partners, Attributes Malicious Cyber Activity and Irresponsible State Behavior to the People's Republic of China.
293 Department of State (2020): The United States Condemns Russian Cyber Attack Against the Country of Georgia.
294 For example, Minister for Foreign Affairs, Minister for Home Affairs and Minister of Defence (2022): Attribution to Russia of malicious cyber activity against Ukraine and DFAT, Australian Government, ACSCe, and Australian Government Department of Home Affairs (2020): UK-US-Canada Joint Advisory on Russia.
295 For example, Minister for Foreign Affairs, Minister for Home Affairs and Minister of Defence (2022): Attribution to Russia of malicious cyber activity against Ukraine.
296 Ministry of Foreign Affairs of Japan (2021): Cases of cyberattacks including those by a group known as APT40 which the Chinese government is behind (Statement by Press Secretary YOSHIDA Tomoyuki).
297 Minister for Foreign Affairs, Minister for Home Affairs and Minister of Defence (2021): Australia joins international partners in attribution of malicious cyber activity to China and Minister for Foreign Affairs, Minister for Home Affairs and Minister of Defence (2022): Attribution to Russia for malicious cyber activity against European networks.
298 For example, DOJ (2018): Chinese Intelligence Officers and Their Recruited Hackers and Insiders Conspired to Steal Sensitive Commercial Aviation and Technological Data for Years and The White House (2021): The United States, Joined by Allies and Partners, Attributes Malicious Cyber Activity and Irresponsible State Behavior to the People's Republic of China. One alert also included an extensive list on previously attributed activity to North Korea (Departments of State, the Treasury, and Homeland Security, and FBI (2020): Guidance on the North Korean Cyber Threat).
299 For example, NCCIC (2017): Petya Ransomware and DHS and FBI (2018): Indicators Associated With WannaCry Ransomware.

Cyber Norms and International Commitments

Especially when issuing OPPAs in the form of statements, focus countries have sometimes resorted to references to UN cyber norms,[300] international commitments, or international law as part of their reasoning. Corresponding references can facilitate the practical interpretation of these commitments and identify specific activities that states perceive are countering them. Applying these abstract formulations to particular operations can provide insight into national understandings of individual norms and rules. This is especially relevant in times when some states express the position that accountability for activities in cyberspace only exists once states have agreed on a dedicated international treaty on information security.[301] Acting on this policy option in the affirmative can thus help advance the implementation of the framework of responsible state behavior as well as the enforcement of other commitments in practice.

Across focus countries' OPPA practices, references to the framework of responsible state behavior increased, but remained limited overall. All states (Germany via the EU[302]), included either **indirect** or **explicit references to UN cyber norms** since 2018 (Australia, Japan, and the U.S.) and 2021 (EU), yet, not all countries employed them similarly. The U.S. included references to cyber norms in all types of communication channels, with an emphasis on statements, and the others have done so exclusively in the framework of political channels. Especially in the beginning, focus countries—excluding Australia—mostly made indirect references.[303] Since then, all focus countries except Japan have tended toward establishing more explicit connections to UN cyber norms.[304] Australia,[305] the U.S.,[306] and the EU[307]

300 UNGA (2015): Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (A/70/174).

301 Permanent Mission of the Russian Federation to the United Nations (2023): Statement by the Representative of the Russian Federation at the Fourth Session of the UN Open-Ended Working Group on Security of and in the Use of ICTs 2021-2025.

302 Germany has not included references to either cyber norms or international law in its OPPAs issued at national capacity.

303 For example, the U.S. has pointed out "commitment[s] to act responsibly in cyberspace" (Department of State (2018): Joint Statement by Secretary of State Michael R. Pompeo and Secretary of Homeland Security Kirstjen Nielsen: Chinese Actors Compromise Global Managed Service Providers), Japan noted that "all the G20 members [... would be] required to take responsible actions [emphasis added] as a member of the international community" (Ministry of Foreign Affairs of Japan (2018): Cyberattacks by a group based in China known as APT10 (Statement by Press Secretary Takeshi Osuga)), or the EU has underlined a "pattern of irresponsible behaviour in cyberspace" (Council of the European Union (2022): Russian cyber operations against Ukraine: Declaration by the High Representative on behalf of the European Union).

304 For example, in 2021, the U.S. provided insights into its interpretation of normative red lines by indicating that the "the international community [would have] laid out clear expectations and guidelines for what constitutes responsible behavior in cyberspace. Responsible states do not indiscriminately compromise global network security nor knowingly harbor cyber criminals – let alone sponsor or collaborate with them" (Department of State (2021): Responding to the PRC's Destabilizing and Irresponsible Behavior in Cyberspace).

305 Minister for Foreign Affairs (2020): Attribution of malicious cyber activity in Georgia to Russian Military Intelligence.

306 Department of State (2018): Joint Statement by Secretary of State Michael R. Pompeo and Secretary of Homeland Security Kirstjen Nielsen: Chinese Actors Compromise Global Managed Service Providers.

307 Council of the European Union (2021): Declaration by the High Representative on behalf of the European Union on respect for the EU's democratic processes.

also called on the attributed actor to adhere to and fulfill respective commitments. Additionally, Australia extended this plea to the international community in a few instances.[308]

Despite these increasingly specific references to UN cyber norms, focus countries have only once pointed to a particular **non-compliance**. Following the cyber operation targeting Albanian government networks in 2022, the U.S. noted that "Iran's conduct disregards norms of responsible peacetime State behavior in cyberspace, which includes a norm on refraining from damaging critical infrastructure that provides services to the public."[309] It went on to underline that it considers Iran's compliance with the norm to be impaired given that "Albania views impacted government networks as critical infrastructure."[310] Close to mentioning a specific non-compliance, EU declarations on the Microsoft Exchange exploitation, the Ghostwriter operation, and the operation against the KA-SAT network highlighted that the attributed behavior was "undertaken in contradiction with the norms of responsible state behavior."[311] Increased references to cyber norms, especially when outlining instances of non-compliance, are desirable to advance the consolidation of shared understandings. At the same time, it must be acknowledged that states may also deliberately seek ambiguity in this respect. This is because, for instance, states may fear that the specification of any red lines could result in subsequent operations occurring precisely below that threshold.

In addition to UN cyber norms, Australia, Japan, and the U.S. also **referred to other bilateral or international commitments**, focusing primarily on intellectual property theft. For instance, Australia,[312] Japan,[313] and the U.S.[314] either referenced or claimed that China violated a G20 commitment "prohibiti[ng] ICT enabled theft

308 For example, Minister for Foreign Affairs, Minister for Home Affairs and Minister of Defence (2022): Attribution to Russia of malicious cyber activity against Ukraine.
309 The White House (2022): Statement by NSC Spokesperson Adrienne Watson on Iran's Cyberattack against Albania.
310 The White House (2022): Statement by NSC Spokesperson Adrienne Watson on Iran's Cyberattack against Albania.
311 Council of the European Union (2021): China: Declaration by the High Representative on behalf of the European Union urging Chinese authorities to take action against malicious cyber activities undertaken from its territory; Council of the European Union (2021): Declaration by the High Representative on behalf of the European Union on respect for the EU's democratic processes and Council of the European Union (2022): Russian cyber operations against Ukraine: Declaration by the High Representative on behalf of the European Union.
312 For example, Minister for Foreign Affairs, Minister for Home Affairs and Minister of Defence (2021): Australia joins international partners in attribution of malicious cyber activity to China.
313 For example, Ministry of Foreign Affairs of Japan (2018): Cyberattacks by a group based in China known as APT10 (Statement by Press Secretary Takeshi Osuga).
314 For example, Department of State (2018): Joint Statement by Secretary of State Michael R. Pompeo and Secretary of Homeland Security Kirstjen Nielsen: Chinese Actors Compromise Global Managed Service Providers.

of intellectual property,[315] to which Australia also added its subsequent bilateral reaffirmation.[316]

Differing from advancing references to cyber norms within the practices of the four focus countries, references to **international law** remain rare and subtle, and none of the OPPA practices analyzed outlined a specific violation of international law. All focus countries sometimes included indirect references by mentioning either the rule of law or the rules-based international order.[317] Australia is the only focus country to have explicitly referenced international law—however, it also did not go into further detail.[318]

Convergence among Focus Countries

Most focus countries' OPPAs provided reasons as to why an operation was attributed that matched at least one of the identified parameters. States thus appear to assent that at least ideally, OPPAs should include some form of reasoning for why an OPPA is being pursued. At the same time, focus countries did not seem to hold clear preferences regarding whether this should come in the form of outlining the severity of the operation, formulating policy objectives, linking it to general policy, referencing prior OPPAs, or alluding to international commitments. Of these, focus countries most often pointed to the severity of the operation attributed, followed by the formulation of policy objectives. In recent years, focus countries' OPPAs increasingly brought up cyber norms. In comparison to these three parameters, explicit links to national (attribution) policies and/or prior OPPAs across cases were established less consistently and widely across cases.

315 Ministry of Foreign Affairs of Japan (2018): Cyberattacks by a group based in China known as APT10 (Statement by Press Secretary Takeshi Osuga). Australia emphasized that respective "commitments [would have been] agreed by G20 Leaders in 2015" (Minister for Foreign Affairs and Minister for Home Affairs (2018): Attribution of Chinese cyber-enabled commercial intellectual property theft) and the U.S. alluded that China would have made respective commitments in both the G20 as well as the the Asia-Pacific Economic Cooperation (Department of State (2018): Joint Statement by Secretary of State Michael R. Pompeo and Secretary of Homeland Security Kirstjen Nielsen: Chinese Actors Compromise Global Managed Service Providers).

316 Minister for Foreign Affairs and Minister for Home Affairs (2018): Attribution of Chinese cyber-enabled commercial intellectual property theft.

317 For example, an EU declaration mentioned the "rule of law" (Council of the European Union (2021): Declaration by the High Representative on behalf of the European Union expressing solidarity with the United States on the impact of the SolarWinds cyber operation), Japan once underlined that its support for the OPPA practices of other states would be an "express[ion of its] determination to uphold the rules-based international order in cyberspace" (Ministry of Foreign Affairs of Japan (2021): Cases of cyberattacks including those by a group known as APT40 which the Chinese government is behind (Statement by Press Secretary YOSHIDA Tomoyuki)), or the U.S. noted that it would "not bring the rule of law to cyberspace until governments refuse to provide safe harbor for criminal hacking within their borders" (DOJ (2020): Two Iranian Nationals Charged in Cyber Theft Campaign Targeting Computer Systems in United States, Europe, and the Middle East).

318 For example, Minister for Foreign Affairs (2020): Attribution of malicious cyber activity in Georgia to Russian Military Intelligence.

4. Sharing Perspectives on Official Public Political Attribution with Other States

In addition to conducting individual OPPAs, states may also be interested in sharing and disseminating perspectives on their OPPA policies with and among other states. Especially when states hold preferences about how to conduct OPPAs, they can be expected to be interested in sharing these understandings with other states, the international community as a whole, or even the public. In other words, as a former U.S. diplomat put it, if states are interested in shaping respective discussions, they need to engage in "attribution diplomacy."[319] It can be assumed that many, if not most, of the respective diplomatic exchanges happen behind closed doors. Thus, it must be acknowledged that the publicly accessible information very likely only reflects a small portion of actual state practices and states probably choose to publicize only parts or aspects in their particular interest.

Focus countries have pursued at least four pathways to share their perspectives on OPPA:

1. Via **agenda-setting** activities,
2. By **sharing information** about the national approach and policy on attribution,
3. By **building coalitions** with like-minded states, and
4. By conducting **cyber capacity-building** (CCB) activities with CCB partner states.

Table 8: Pursued Pathways by Focus Countries

Agenda-setting	Information-sharing	Coalition-building	Capacity-building
AU DE JP US	AU DE JP US	AU DE JP US	US

Their pursuit is not mutually exclusive given possibly overlapping objectives. Also, international coordination on individual OPPAs as discussed in Section 3.5 may contribute to sharing one's own perspective with other states and soliciting their support.

319 Department of State (2020): Responding to Modern Cyber Threats with Diplomacy and Deterrence. In International Relations literature, this behavior is referred to as "norm entrepreneurship" (see further Martha Finnemore and Kathryn Sikkink (1998): International Norm Dynamics and Political Change, in: International Organization 52 (4), pp. 887–917 and Martha Finnemore and Duncan B. Hollis (2016): Constructing Norms for Global Cybersecurity, in: The American Journal of International Law 110 (3), pp. 425-479).

Agenda-setting activities, that is, bringing the issue to the attention of other actors, can take the elementary forms of raising awareness of the concept of public attribution of cyber operations to calling for international discussions or joint activities. Focus countries did so particularly within the framework of the UN. The UN Open-ended Working Group on security of and in the use of information and communications technologies (OEWG) constitutes the most prominent forum for respective focus countries' practices. It also represents a particularly promising forum for states seeking to engage in agenda-setting activities because it is open to all 193 UN Member States, holds public sessions, and has a track record of high and continuously increasing Member State participation. During formal sessions of the UN OEWG, all focus countries raised the issue of (public) attribution.[320] For instance, both Australia[321] and Germany[322] referred to their own past OPPAs. Germany also raised the need for "further work on how to conduct attribution of cyber incidents,"[323] and the U.S. called for "additional guidance on this important topic."[324] Japan also touched upon the issue within a UN Security Council meeting discussing cybersecurity,[325] and Germany[326] and Australia[327] included it in national contributions to a dedicated, thematic annual report of the UN. States also brought up the issue of attribution in ministerial meetings of the Group of Seven (G7)[328], the Five Eyes intelligence cooperation,[329] or a strategic trilateral dialogue between Australia, Japan, and the U.S.[330] There is no public indication as to whether any

320 Australia: Australia (2023): Statement by the Representative of Australia to the Fourth Substantive Session of the Open Ended Working Group on Security of and in the Use of ICTs (March 2023). Existing and emerging threats, Australia (2022): Statement by the Representative of Australia to the Second Substantive Session of the Open Ended Working Group on Security of and in the Use of ICTs (March 2022). Existing and emerging threats, Australia (2022): Statement by the Representative of Australia to the Second Substantive Session of the Open Ended Working Group on Security of and in the Use of ICTs (March 2022). International Law, Australia (2020): OEWG Virtual Meeting: 2 July 2020 Australian Intervention, and DFAT (2020): Australia's response to the OEWG Pre-draft Report – April 2020; Germany: Germany (2022): German Statement at the July OEWG, Agenda Item 5, Section B, Germany (2022): German Statement at the March OEWG, Agenda Item 5a, and Germany (2021): Comments by Germany on the OEWG Zero Draft Report; Japan: Japan (2022): International Law; and U.S.: U.S. (2022): United States remarks for March 2022 session of the OEWG, as prepared.

321 Australia (2022): Statement by the Representative of Australia to the Second Substantive Session of the Open Ended Working Group on Security of and in the Use of ICTs (March 2022). Existing and emerging threats and Australia (2023): Statement by the Representative of Australia to the Fourth Substantive Session of the Open Ended Working Group on Security of and in the Use of ICTs (March 2023). Existing and emerging threats.

322 Germany (2022): German Statement at the March OEWG, Agenda Item 5a.

323 Germany (2022): German Statement at the March OEWG, Agenda Item 5a.

324 U.S. (2022): United States remarks for March 2022 session of the OEWG, as prepared.

325 Ministry of Foreign Affairs Japan (2021): Statement by Mr. Akahori Takeshi, Ambassador for United Nations Affairs and Cyber Policy of the Ministry of Foreign Affairs of Japan, at the United Nations Security Council Open Debate on Cyber Security.

326 UNGA (2011): Developments in the field of information and telecommunications in the context of international security. Report of the Secretary-General (A /66/152).

327 UNGA (2022): Developments in the field of information and telecommunications in the context of international security, and advancing responsible State behaviour in the use of information and communications technologies. Report of the Secretary-General (A/77/92).

328 Government of Canada (2018): G7 foreign ministers' communiqué.

329 Department of Home Affairs (2018): Five country ministerial 2018.

330 Department of State (2019): Trilateral Strategic Dialogue Joint Ministerial Statement, August 1, 2019.

of the focus countries raised the issue in other bilateral settings, such as cyber dialogues or consultations.

Information-sharing activities can complement agenda-setting objectives. Nevertheless, there are limits, as states cannot be expected to "provide complete transparency on their own guiding principles for public attribution"[331] due to the widespread confidentiality of internal decision-making processes. However, sharing information on the national approach and policy on attribution can be beneficial, as it may influence how other states perceive individual OPPA practices. Such information can provide insights for contextualization, for example, how a state reaches an attribution decision or its respective priorities. In like-minded circles, increased information-sharing might, over the medium or long term, also facilitate increased international coordination on OPPAs as an output of enhanced confidence-building.

In this respect, the practices of the four focus countries indicate a trend toward being more open, as they have used a variety of mediums for that purpose. For instance, all states have included information on their perspective on attribution within national publications, such as annual intelligence reports,[332] annual disarmament reports,[333] annual Ministry of Foreign Affairs reports,[334] cyber-related threat reports,[335] or national papers on either the implementation of the UN GGE cyber norms[336] or specifically the attribution of cyber operations.[337] Worth mentioning is a position paper by German Cyber Ambassador Regine Grienberger, in her personal capacity, in which she, inter alia, shared experiences with and lessons learned from Germany's national attribution processes.[338] All focus countries also published national position papers on the applicability of international law that

331 Florian Egloff and Max Smeets (2021): Publicly attributing cyber attacks: a framework, in: Journal of Strategic Studies 46 (3), pp. 502-533.
332 ACSC (2016): ACSC Threat Report 2016; Public Security Intelligence Agency (2022): Overview of Threats in Cyberspace 2022.
333 Auswärtiges Amt (2022): Jahresabrüstungsbericht 2021.
334 Ministry of Foreign Affairs Japan (2022): Chapter 3. Japan Strengthening Its Presence in the International Community.
335 Public Security Intelligence Agency (2022): Overview of Threats in Cyberspace 2022.
336 DFAT (2020): Annex B. Australian Implementation of Norms of Responsible State Behaviour in Cyberspace. Regarding its implementation of norm b, Australia, for example, noted that: "During a national cyber incident, the Australian Government's first priority is to mitigate the impact. Attribution of malicious activity is then necessary to enable a range of strategic response options. Depending on the seriousness and nature of an incident, Australia has the capability to attribute malicious cyber activity ranging from the broad category of adversary through to specific states and individuals. Australia has a well-developed process to guide and inform a decision by the Australian Government to make a public or private attribution disclosure. This process includes, but is not limited to, considering all relevant information, including the larger context of the event, the challenges of attribution in the ICT environment and the nature and extent of the consequences."
337 ODNI (2018): A Guide to Cyber Attribution and Regine Grienberger (2023): Cyberangreifer benennen, globale Normen stärken: Erfahrungen mit dem Attributionsverfahren der Bundesregierung, Bundesakademie für Sicherheitspolitik.
338 Regine Grienberger (2023): Cyberangreifer benennen, globale Normen stärken: Erfahrungen mit dem Attributionsverfahren der Bundesregierung, Bundesakademie für Sicherheitspolitik.

touch upon the issue of attribution.[339] Additionally, national government officials raised the issue within speeches, referencing previous activities, for example.[340]

On a strategic level, Australia, Germany, Japan, and the U.S. laid out attribution-related policy priorities in the framework of their national security strategies,[341] national cybersecurity strategies,[342] or other thematic strategies.[343] Most likely less in the public spotlight of other states, Australia has also provided input and answered questions relating to, among other issues, its national attribution process or past Australian attributions in the context of publicly transcribed domestic parliamentary debates.[344] Germany[345] and Australia[346] also publicly acknowledged that they have shared their confidential national attribution processes with other countries. The German Cyber Ambassador also shared that Germany disclosed its analysis of the Viasat incident and explained its response with and to other states within the framework of the OSCE a week after it had communicated its OPPA.[347]

Australia and the U.S. also provide a publicly available list of their past OPPA practices in varying formats.[348] While the initial setting up of such an overview on their website does not require many resources, continuous updates are required.

339 DFAT (2020): Annex A. 2017 - Australia's Position on the Application of International Law to State Conduct in Cyberspace; Federal Government (2021): On the Application of International Law in Cyberspace; Ministry of Foreign Affairs of Japan (2021): Basic Position of the Government of Japan on International Law Applicable to Cyber Operations, and UNGA (2021): Official compendium of voluntary national contributions on the subject of how international law applies to the use of information and communications technologies by States submitted by participating governmental experts in the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security established pursuant to General Assembly resolution 73/266 (A /76/136).

340 DFAT (2019): Address to the Lowy Institute; DFAT (2019): The Lowy Institute International Cyber Engagement Q and A; Auswärtiges Amt (2022): Rede von Außenministerin Annalena Baerbock auf der Konferenz „Shaping Cyber Security" in Potsdam; Ministry of Foreign Affairs Japan (2020): Speech at 10th International Cybersecurity Symposium; Department of State (2020): Cyberspace Security Diplomacy: Deterring Aggression in Turing's Monument; and Department of State (2020): Responding to Modern Cyber Threats with Diplomacy and Deterrence.

341 Federal Government (2023): Robust. Resilient. Sustainable. Integrated Security for Germany. National Security Strategy; Cabinet Secretariat (2022): National Security Strategy of Japan, and The White House (2022): National Security Strategy.

342 DFAT (2021): Australia's International Cyber and Critical Technology Engagement Strategy; DFAT (2017): Australia's International Cyber Engagement Strategy; BMI (2021): Cyber Security Strategy for Germany 2021; The White House (2023): National Cybersecurity Strategy; and The White House (2018): National Cyber Strategy of the United States of America.

343 Federal Government (2023): Strategy on China.

344 For example, Australian Foreign Affairs, Defence And Trade Legislation Committee (2019): Friday, 5 April 2019, Official Committee Hansard and Australian Foreign Affairs, Defence And Trade Legislation Committee (2017): Wednesday, 31 May 2017, Official Committee Hansard.

345 As German motivations behind sharing the process, Ambassador Grienberger enumerated the creation of transparency, the possibility to influence expectations, and, in the long run, arriving at generally accepted minimum standards for attribution decisions (Regine Grienberger (2023): Cyberangreifer benennen, globale Normen stärken: Erfahrungen mit dem Attributionsverfahren der Bundesregierung, Bundesakademie für Sicherheitspolitik).

346 Australian Foreign Affairs, Defence And Trade Legislation Committee (2021): Thursday, 3 June 2021, Official Committee Hansard.

347 Regine Grienberger (2023): Cyberangreifer benennen, globale Normen stärken: Erfahrungen mit dem Attributionsverfahren der Bundesregierung, Bundesakademie für Sicherheitspolitik.

348 The need for a "repository of public attribution efforts" has also been discussed by the Global Forum of Cyber Expertise (GFCE (2021): The Global Cyber Capacity Building Research Agenda 2022 - 2023).

Rather than general information about national attribution policy, such a list shows how states have implemented these policies in practice, which is essential for sharing perspectives on OPPA. Australia has done so for OPPAs communicated via political channels,[349] whereas the U.S. has maintained both country-specific overviews of alerts, advisories, or reports outlining respective malicious behaviors for four perpetrator states[350] and an overview of cyber-related sanctions issued.[351]

In addition to sharing information and putting the issue on the agenda, the focus countries engaged in **coalition-building activities** with like-minded states. Corresponding activities can take place at various levels of formalization and may provide connecting points and fora for further coordination and trusted avenues to share information and exchange views. In turn, they can also facilitate the degree of coordination when it comes to individual OPPA practices. To this end, focus countries have convened or participated[352] in like-minded international discussions. For instance, through its 2018 National Cyber Strategy, the U.S. established a so-called "Cyber Deterrence Initiative" seeking to "work with like-minded states to coordinate and support each other's responses to significant malicious cyber incidents, including through intelligence sharing, buttressing of attribution claims, public statements of support for responsive actions taken, and joint imposition of consequences against malign actors."[353] In September 2019, all four focus countries—with others—pledged that they would, inter alia, "when necessary, [...] work together on a voluntary basis to hold states accountable when they act contrary to this framework"[354] in the framework of a joint statement on advancing responsible state behavior in cyberspace. Nevertheless, despite these announcements and agreements, little is known or has been disclosed about how these commitments have been or are implemented in practice. Moreover, after peaking in 2019, there has since been a remarkable decrease in publicly available information on similar coalition-building activities.

349 DFAT (n.d.): Attribution. A similar list of prior OPPA practices was also incorporated by Australia in its 2021 International Cyber and Critical Tech Engagement Strategy (DFAT(2021): Australia's International Cyber and Critical Technology Engagement Strategy). Aside from the four focus countries, also Canada, for example, provides a similar list (Government of Canada (n.d.): Malicious cyber activity response).

350 CISA (n.d.): China Cyber Threat Overview and Advisories; CISA (n.d.): Russia Cyber Threat Overview and Advisories; CISA (n.d.): North Korea Cyber Threat Overview and Advisories; and CISA (n.d.): Iran Cyber Threat Overview and Advisories.

351 Department of State (n.d.): Cyber Sanctions. Yet, not all of the sanctions listed in this overview represent an OPPA as defined in this analysis, as, for example, cybercriminal groups feature among sanctioned entities where no nexus to the involvement of another state is being drawn. This list not only details past OPPA practices but also includes policy foundations and applicable legislation.

352 In June 2023, all focus countries participated in "international discussions on collective responses to malicious cyber activity" hosted by Canada (Government of Canada (2023): Chair statement: International discussions on collective responses to malicious cyber activity).

353 The White House (2018): National Cyber Strategy of the United States of America.

354 Department of State (2019): Joint Statement on Advancing Responsible State Behavior in Cyberspace.

Focus countries have also shared preferences about the conduct of OPPAs through international **capacity-building activities**. While many states have highlighted the importance of capacity-building related to attribution,[355] only the U.S. has publicly shared that they implemented respective activities in practice. In 2021, they hosted a "first-of-its kind course for policymakers worldwide on the policy and technical aspects of publicly attributing cyber incidents" at the George C. Marshall Center in Germany[356]. A total of 50 policymakers from all over the world attended the course, which provided "capacity-building assistance to help partner nations more effectively organize, engage in discussions, and take appropriate national action on public attribution when responding to significant cyber incidents."[357]

355 For example, U.S. (2022): United States remarks for March 2022 session of the OEWG, as prepared; Permanent Mission of Thailand to the United Nations (2023): Statement by Mr. Krirkrit Ponlakhetpaiboon [...], Agenda item 5: Discussions on substantive issues contained in paragraph 1 of General Assembly resolution 75/240 on how international law applies to the use of information and communications technologies by States at the fourth substantive session of the UN OEWG 2021-2025; Regine Grienberger (2023): Cyberangreifer benennen, globale Normen stärken: Erfahrungen mit dem Attributionsverfahren der Bundesregierung, Bundesakademie für Sicherheitspolitik; and GIP Digital Watch (2022): UN OEWG 2021-2025 – Confidence building measures.

356 The White House (2021): Fact Sheet: Imposing Costs for Harmful Foreign Activities by the Russian Government, also reiterated in Department of State (2021): Holding Russia To Account.

357 George C. Marshall European Center for Security Studies (2021): PCSS: Public Attribution for Policy Makers.

5. Conclusion and Outlook

Given the prevalence of cyber operations, pursuing OPPAs will continue to constitute a central policy instrument for states to respond to them. Against this backdrop, it is necessary to not only discuss whether and under which circumstances to use OPPA, but also how to do so. This paper conducted a comparative analysis examining how states have publicly disclosed information tying a cyber operation to another state through official channels, also referred to as OPPA. To this end, this analysis focused on what, how, and why four states—Australia, Germany, Japan, and the U.S.—officially and publicly attributed cyber operations seeking to identify similarities and differences in their approaches. Based on their practices, 13 parameters with corresponding options were analyzed that serve to explore areas of convergence and divergence among the focus countries.

Overview of Parameters

1. Choice of communication channel
2. Selection of government entity(ies) communicating the OPPA
3. Factual description of the operation attributed
4. Provision of details on the attributed actor
5. Inclusion of a message to the attributed actor
6. Provision of or reference to evidence
7. Inclusion of estimative probability
8. Engagement in international cooperation and coordination efforts
9. Specification of the severity of the operation attributed
10. Formulation of policy objectives pursued with OPPA
11. Linkage to national (attribution) policy
12. Inclusion of reference to prior OPPAs
13. Reference to cyber norms or other commitments

In using these parameters as analytical categories for comparison, this analysis has found that:

1. **Communication channels and designated government entities vary across countries and over time.** This is important, as both parameters may pre-determine or influence how many of the other parameters will be addressed and impact the OPPA's framing and external reception. It may also coincide with the pursuit of different policy objectives as focus countries have used political, technical, as well as criminal law and economic sanctions channels to communicate their OPPAs. Focus countries' practice varies to the extent that some states have prioritized particular channels at least for a period over time, others have diversified their usage of channels over the years, while one state has employed all three channels. Which government entities are designated as communicator(s)—attributing actors—of the OPPA depends highly on national institutional set-ups. The four focus countries coincide in that particularly their Ministries of Foreign Affairs and national cybersecurity, intelligence, or law enforcement agencies have assumed that role.
2. **OPPAs always provide details on the operations attributed.** Many OPPAs particularly emphasize targets and/or victims of the operation, followed by the timing and duration of the operation. Across cases, the damage and harm caused by the operation has been increasingly, but less often, alluded to.
3. **OPPAs differ in how they specify the attributed actor and sometimes include a message addressed to the actor.** Focus countries' OPPAs have always attributed authorship for the outlined behavior. Due to the variety of potential constellations between an attributed government and the perpetrator(s) of a cyber operation, states often have some political leeway regarding how to name the other state—the attributed actor—deemed politically responsible. In this respect, focus countries have employed seven different levels of specificity, ranging from individuals working for organs or entities of a particular state to the least specific exclusive reference to an APT group. The chosen channel can affect what level is being used, since OPPAs conducted via technical, criminal law, and economic sanctions channels generally attribute at a higher specificity than their political counterparts, which show greater overall variety. Comparing the employed levels of specificity over time suggests that states have tended to be more specific in recent years, possibly also due to maturing attribution policies and capacities. In addition to naming the attributed actor at any level of specificity, focus countries have sometimes also used their OPPAs to publicly appeal to the attributed actor to cease the operation attributed expressed that they reserved the right to initiate further consequences.

4. **Only some OPPAs mention evidentiary information and estimative probability.** As part of their OPPAs, focus countries have occasionally—but slightly increasing over time—mentioned the existence or reliance on technical evidence, referred to governmental sources of evidence, or hinted at commercial reporting informing their attribution decisions. This confirms that the choice of communication channel is essential, since some channels may either necessitate or be more prone to the inclusion of evidence, as well as levels of confidence or likelihood. More rarely altogether, yet particularly in the form of technical channels, focus countries have also provided specific technical information substantiating their OPPAs—possibly in an effort to point out that their political attributions were based on a preceding technical attribution.
5. **States increasingly coordinate their OPPAs with like-minded countries.** Focus countries have internationally coordinated their OPPAs in three main ways, in decreasing order of the degree of coordination required: participating in internationally coordinated attributions, supporting the OPPA practice of another state with or without their own attribution assessment, and retrospectively endorsing the OPPA of another state. In recent years, focus countries have predominantly made use of the first type in the form of joint statements or advisories, either through more ad hoc, like-minded constellations or institutionalized processes within the EU. As some states have also referred to evidence of international origin or OPPAs of other states informing their OPPA, focus countries appear to agree that, if possible, states should at least consult like-minded states before publicizing their OPPAs.
6. **States regularly explain why they attribute, pointing to the operation, their policies, and/or international commitments.** Most focus countries' OPPAs provided a glimpse into their reasoning as to why an operation is being attributed, particularly when using political channels. Yet, focus countries do not seem to hold clear preferences on whether this should be done in the form of outlining the severity of the operation, formulating policy objectives, linking it to general policy, referencing prior OPPAs, or alluding to international commitments, as their practices do not indicate a consistent tendency in this regard. Of the five parameters and across OPPAs, specifications of the effect and risks posed by the operation, the formulation of policy objectives, and, increasingly, the reference to international commitments have been most significant in terms of quantity.

Given the varied ways in which states carried out their official public political attributions, the degree and scope of international convergence regarding how to conduct official public political attribution is limited among the four states at present.

At the same time, their practices also suggest three developments that merit further observation in terms of possibly enhancing convergence in the future:

- Increased domestic inter-agency coordination through the joint issuance of an OPPA by multiple domestic authorities and the codification of national attribution processes,
- The combination of political statements and technical advisories to communicate and substantiate an OPPA, and
- Progressively expanding references to cyber norms.

While these developments also indicate an augmented regularization and structurization of OPPA policies within governments, it is too early to say whether a particular convergence can be inferred from state practices.

With more public attributions likely on the horizon, more states may—actively or incidentally—shape normative understandings of responsible attribution. States seeking to demonstrate that they act responsibly when publicly attributing cyber operations may want to consider building shared understandings on this issue with other states. For this purpose, focus countries have engaged in agenda-setting, proactive information-sharing, coalition-building, and capacity-building activities to initiate or deepen a debate on responsible OPPA. The more a state engages in these activities, the more it can be considered to be interested in spreading ideas about how OPPAs should be conducted. The respective public engagements of the focus countries match the quantitative distribution of OPPAs overall. Accordingly, the U.S. displays a strong interest in shaping understandings about OPPA. Australia and recently also Germany have been active to some extent, while Japan has only shown a few similar actions.

Given that many states are either regularizing or establishing their OPPA policies and processes at the moment, the framework of parameters and options presented in this analysis can aid decision-makers in developing an attribution policy or increasing consistency across attributions. It may likewise be applied to other states to shed light on the extent to which they (dis)agree on what constitutes responsible attribution. Accordingly, the framework may help guide international debate and inter-state exchanges on the topic, especially in like-minded constellations, and support states' efforts to operationalize UN cyber norm (b).

Even though almost 10 years have passed since the first OPPA, OPPAs still represent a policy instrument that has only recently gained traction and political importance. In the future, the way OPPAs are or should be conducted might become more contested due to an expanding circle of states capable of and interested

in making use of this policy instrument. Therefore, now is a crucial moment for states to discuss best practices and voice preferences regarding how OPPAs should be carried out. For the instrument to mature, a nuanced international policy debate is required, and decision-makers should seek ways to increase convergence, despite, or precisely because of, the topic's sensitivity. Since these understandings can contribute to conflict prevention and stabilization by creating collective expectations as to how OPPAs are to be carried out responsibly, states should actively consider what part they can or want to play in their elaboration—either implicitly through their OPPA practices or explicitly through the pursuit of pathways to spread ideas with and among other states.

Annex

I-IV

Structured by country in alphabetical order, the annex includes country-specific overviews in the form of 'OPPA Profiles' of the four selected focus countries and a list with sources of their OPPA practices. It also details attributing and attributed actors of a specific OPPA. The OPPA Profiles build upon the analytical framework comprising parameters and options discussed throughout Chapter 3. Within OPPA profiles, options are highlighted in color when the particular state explicitly employed it as part of its OPPA practice.

I. Australia

OPPA Profile: Australia

Parameters	Options
 Choice of communication channel	Choice of technical communication channel
	Choice of political communication channel
	Choice of criminal law or economic sanctions channel
	Combination of various communication channels as part of a coordinated attribution practice
 Selection of government entity(ies) communicating the OPPA	Designation of Ministry of Foreign Affairs, national cybersecurity/intelligence/law enforcement agency, or another government entity as communicator of the OPPA
	Joint issuance of OPPA by multiple domestic authorities
 Factual description of the operation attributed	Indication of (type of) target/victim and/or its location
	Indication of date when the operation attributed took place and, if applicable, its duration
	Indication of harm and/or damage caused by the operation attributed

Parameters	Options
 Provision of details on the attributed actor	Reference to individuals working for organs or entities of a particular state
	Reference to organs or entities of a particular state
	Reference to actors operating under the direction of or sponsorship by a specific organ/entity of a particular state
	Reference to actors operating under the direction of or sponsorship by government of a particular state
	Reference to government of a particular state
	Reference to “state X”
	Exclusive reference to a specific APT group
	Additional provision of details about the location out of which the attributed actor has operated
	Additional inclusion of reference to prior activities/operations of attributed actor
 Inclusion of a message to the attributed actor	Appeal to the attributed actor to cease activity(ies) attributed
	Announcement of possible further consequences
 Provision of or reference to evidence	Mentioning of existence or general reliance on technical evidence without further details
	Reference to governmental sources of evidence
	Reference to commercial reporting
	Provision of technical information
 Inclusion of estimative probability	Inclusion of a level of confidence or likelihood
 Engagement in international cooperation and coordination efforts	Participation in internationally coordinated attribution
	Support of OPPA practice by another state with own attribution assessment
	Support of OPPA practice by another state without own attribution assessment
	Retrospective endorsement of an OPPA by another state
	Reference to evidence of international origin or OPPAs of other states
 Specification of the severity of the operation attributed	Indication of effect and/or impact of operation attributed
	Indication of threats and/or risks posed by operation attributed
	Indication of assumed goals of attributed actor

Parameters	Options
 Formulation of policy objectives pursued with OPPA	Exposure of or response to malicious cyber activity
	Imposition of pressure, costs, or consequences
	Provision of information, awareness raising and/or warning of organizations
	Defense and protection of national interests or allies
 Linkage to national (attribution) policy	Reference to national strategies/policy documents
	Mentioning of domestic or international cybersecurity response actions
 Inclusion of reference to prior OPPAs	Inclusion of a reference to own previous OPPA practices in general or to the same attributed actor
 Reference to cyber norms or other commitments	Indirect or explicit reference to UN cyber norms or the framework of responsible state behavior
	Reference to bilateral or international commitments
	Mentioning non-compliance with a specific cyber norm or other commitments

List of Australian OPPA Practices

	Day Month Year	Communication channel	Attributing actor	Attributed actor	Source
			2017		
1	20 December 2017	Statement	Australian Minister for Foreign Affairs	"North Korea"	Minister for Foreign Affairs (2017): Australia attributes WannaCry ransomware to North Korea.
			2018		
2	16 February 2018	Statement	Minister for Law Enforcement and Cyber Security	"Russian state sponsored actors"	Minister for Law Enforcement and Cyber Security (2018): Australian Government attribution of the 'NotPetya' cyber incident to Russia.
3-4	17 April 2018	Statement	Minister for Law Enforcement and Cyber Security	"Russian state-sponsored actors"	Minister for Law Enforcement and Cyber Security (2018): Australian Government attribution of cyber incident to Russia.
		Alert	Australian Cyber Security Centre	"Russian state-sponsored actors"	Australian Cyber Security Centre (2018): Routers targeted: Cisco Smart Install feature continues to be targeted by Russian state-sponsored actors.
5	04 October 2018	Statement	Prime Minister & Minister for Foreign Affairs	"Russian military, and their intelligence arm 'the GRU'"	Prime Minister and Minister for Foreign Affairs (2018): Attribution of a pattern of malicious cyber activity to Russia.
6	05 October 2018	Statement	Minister for Foreign Affairs	"Russia"	Minister for Foreign Affairs (2018): Australia condemns the cyber operations attributed to Russia against the Organisation for the Prohibition of Chemical Weapons (OPCW) and against Malaysian locations participating in the Flight MH-17 investigation as revealed by Dutch and UK authorities overnight.
7	21 December 2018	Statement	Minister for Foreign Affairs & Minister for Home Affairs	"APT10, acting on behalf of the Chinese Ministry of State Security"	Minister for Foreign Affairs and Minister for Home Affairs (2018): Attribution of Chinese cyber-enabled commercial intellectual property theft.
			2019		
			2020		
8	21 February 2020	Statement	Minister for Foreign Affairs	"GRU, Russia's military intelligence service"	Minister for Foreign Affairs (2020): Attribution of malicious cyber activity in Georgia to Russian Military Intelligence.

	Day Month Year	Communication channel	Attributing actor	Attributed actor	Source
9	17 July 2020	Statement	Australian Government Department of Foreign Affairs, Australian Government, Australian Cyber Security Centre, and Australian Government Department of Home Affairs	"Russian actors [...] almost certainly operat[ing] as part of Russian intelligence services"	Department of Foreign Affairs, Australian Government, Australian Cyber Security Centre, and Australian Government Department of Home Affairs (2020): UK-US-Canada Joint Advisory on Russia.
			2021		
10	15 April 2021	Statement	Minister for Foreign Affairs, Minister for Home Affairs & Minister for Defence	"Russian state actors"	Minister for Foreign Affairs, Minister for Home Affairs and Minister of Defence (2021): Attribution of cyber incident to Russia.
11	19 July 2021	Statement	Minister for Foreign Affairs, Minister for Home Affairs & Minister for Defence	"China's Ministry of State Security"	Minister for Foreign Affairs, Minister for Home Affairs and Minister of Defence (2021): Australia joins international partners in attribution of malicious cyber activity to China.
12	17 November 2021	Advisory	Australian Cyber Security Centre (with FBI, CISA, and NCSC)	"Iranian government-sponsored APT group"	Australian Cyber Security Centre et al. (2021): Iranian Government-Sponsored APT Cyber Actors Exploiting Microsoft Exchange and Fortinet Vulnerabilities in Furtherance of Malicious Activities.
			2022		
13	20 February 2022	Statement	Minister for Foreign Affairs, Minister for Home Affairs & Minister for Defence	"Russian Main Intelligence Directorate (GRU)"	Minister for Foreign Affairs, Minister for Home Affairs and Minister of Defence (2022): Attribution to Russia of malicious cyber activity against Ukraine.
14	20 April 2022	Advisory	Australian Cyber Security Centre (with CISA, FBI, NSA, CCCS, NCSC, and NCSC and NCA)	"Russian government"	Australian Cyber Security Centre et al. (2022): Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure.
15	10 May 2022	Statement	Minister for Foreign Affairs, Minister for Home Affairs & Minister for Defence	"Russian military cyber operators"	Minister for Foreign Affairs, Minister for Home Affairs and Minister of Defence (2022): Attribution to Russia for malicious cyber activity against European networks.

	Day Month Year	Communication channel	Attributing actor	Attributed actor	Source
16	14 September 2022	Advisory	Australian Cyber Security Centre (with FBI, CISA, NSA, U.S. Cyber Command Cyber National Mission Force, Department of the Treasury, CCCS, and NCSC)	"APT actors [...] affiliated with the Iranian Government's Islamic Revolutionary Guard Corps"	Australian Cyber Security Centre et al. (2022): Iranian Islamic Revolutionary Guard Corps-Affiliated Cyber Actors Exploiting Vulnerabilities for Data Extortion and Disk Encryption for Ransom Operations.
			2023		
17	09 May 2023	Advisory	Australian Cyber Security Centre (with FBI, NSA, CISA, Cyber National Mission Force, NCSC, CCCS and CSE, and NCSC)	"Center 16 of Russia's Federal Security Service (FSB)"	Australian Cyber Security Centre et al. (2023): Hunting Russian Intelligence "Snake" Malware.

II. Germany

OPPA Profile: Germany

Parameters	Options
 Choice of communication channel	Choice of technical communication channel
	Choice of political communication channel
	Choice of criminal law or economic sanctions channel
	Combination of various communication channels as part of a coordinated attribution practice
 Selection of government entity(ies) communicating the OPPA	Designation of Ministry of Foreign Affairs, national cybersecurity/intelligence/law enforcement agency, or another government entity as communicator of the OPPA
	Joint issuance of OPPA by multiple domestic authorities
 Factual description of the operation attributed	Indication of (type of) target/victim and/or its location
	Indication of date when the operation attributed took place and, if applicable, its duration
	Indication of harm and/or damage caused by the operation attributed
 Provision of details on the attributed actor	Reference to individuals working for organs or entities of a particular state
	Reference to organs or entities of a particular state
	Reference to actors operating under the direction of or sponsorship by a specific organ/entity of a particular state
	Reference to actors operating under the direction of or sponsorship by government of a particular state
	Reference to government of a particular state
	Reference to “state X”
	Exclusive reference to a specific APT group
	Additional provision of details about the location out of which the attributed actor has operated
	Additional inclusion of reference to prior activities/operations of attributed actor
 Inclusion of a message to the attributed actor	Appeal to the attributed actor to cease activity(ies) attributed
	Announcement of possible further consequences

Parameters	Options
 Provision of or reference to evidence	Mentioning of existence or general reliance on technical evidence without further details
	Reference to governmental sources of evidence
	Reference to commercial reporting
	Provision of technical information
 Inclusion of estimative probability	Inclusion of a level of confidence or likelihood
 Engagement in international cooperation and coordination efforts	Participation in internationally coordinated attribution
	Support of OPPA practice by another state with own attribution assessment
	Support of OPPA practice by another state without own attribution assessment
	Retrospective endorsement of an OPPA by another state
	Reference to evidence of international origin or OPPAs of other states
 Specification of the severity of the operation attributed	Indication of effect and/or impact of operation attributed
	Indication of threats and/or risks posed by operation attributed
	Indication of assumed goals of attributed actor
 Formulation of policy objectives pursued with OPPA	Exposure of or response to malicious cyber activity
	Imposition of pressure, costs, or consequences
	Provision of information, awareness raising and/or warning of organizations
	Defense and protection of national interests or allies
 Linkage to national (attribution) policy	Reference to national strategies/policy documents
	Mentioning of domestic or international cybersecurity response actions
 Inclusion of reference to prior OPPAs	Inclusion of a reference to own previous OPPA practices in general or to the same attributed actor

Parameters	Options
 Reference to cyber norms or other commitments	Indirect or explicit reference to UN cyber norms or the framework of responsible state behavior
	Reference to bilateral or international commitments
	Mentioning non-compliance with a specific cyber norm or other commitments

List of German OPPA Practices

	Day Month Year	Communication channel	Attributing actor	Attributed actor	Source
			2015		
1-4	30 June 2015	Report	Bundesamt für Verfassungsschutz	"im Fokus chinesischer Angreifer" [in the focus of Chinese attackers, own translation]	Bundesministerium des Innern (2015): Verfassungsschutzbericht 2014 [in German only].
			Bundesamt für Verfassungsschutz	"mit mutmaßlich nachrichtendienstlichem Hintergrund einem chinesischen Angreifer zuzuordnen" [attributed to a Chinese attacker with suspected intelligence background, own translation]	
			Bundesamt für Verfassungsschutz	"Im chinesischen Aufklärungsinteresse stehen zudem weiterhin [...] Nachdem das BfV im Jahr 2014 von einem großen Unternehmen detailliert über einen „Elektronischen Angriff" informiert worden war, ist es gelungen, die Angriffsinfrastrukturen aufzuklären und weitere Informationen zu gewinnen" [Chinese intelligence interests also continue to include [...] After the BfV was informed in detail by a large company in 2014 about an 'electronic attack' it succeeded in clarifying the attack infrastructures and gain further information, own translation]	
			Bundesamt für Verfassungsschutz	"geht das BfV von einer russischen nachrichtendienstlichen Angriffsoperation aus" [the BfV assumes a Russian intelligence attack operation, own translation]	
			2016		
5	11 May 2016	Alert	Bundesamt für Verfassungsschutz	"Snake"	Bundesamt für Verfassungsschutz (2016): BfV Cyber-Brief Nr. 02/2016 [in German only].
6-8	28 June 2016	Report	Bundesamt für Verfassungsschutz	"APT-Angriffskampagne [...] Die Ermittlungen lassen auf eine Steuerung durch russische staatliche Stellen schließen" [APT attack campaign [...] the investigation suggests control by Russian state entities, own translation]	Bundesministerium des Innern (2016): Verfassungsschutzbericht 2015 [in German only].
			Bundesamt für Verfassungsschutz	"Angriffskampagne mit einem mutmaßlich chinesischen Hintergrund" [Attack campaign with a suspected Chinese background, own translation]	
			Bundesamt für Verfassungsschutz	"mit hoher Wahrscheinlichkeit einem iranischen Nachrichtendienst zuzuordnen sind" [attributable to an Iranian intelligence service with high confidence, own translation]	

	Day Month Year	Communication channel	Attributing actor	Attributed actor	Source
			2017		
9	07 January 2017	Quote	President of Bundesamt für Verfassungsschutz	"APT28 [... es] liegen Indizien vor, die auf russische Quellen hindeuten" [APT28...there is evidence pointing to Russian sources, own translation]	dpa (2017): Geheimdienste: Putin ließ US-Wahl durch Hacker beeinflussen. [in German only]
10-11	08 February 2017	Governmental response to parliamentary inquiry	Federal Government	"APT29"	German Bundestag (2017): Antwort der Bundesregierung auf die Kleine Anfrage: Ermittlungen zu angeblich russischen Cyberangriffen (Drucksache 18/11106) [in German only].
			Federal Government	"APT29"	
12	23 May 2017	Alert	Bundesamt für Verfassungsschutz	"chinesische Angreifer-Gruppierung [... bekannt] unter anderem unter den Namen APT 10, Menupass Team und Stone Panda" [Chinese attacker group known under the names APT 10, Menupass Team and Stone Panda, among others, own translation]	Bundesamt für Verfassungsschutz (2017): BfV Cyber-Brief Nr. 02/2017 [in German only].
			2018		
13	11 April 2018	Quote	President of Bundesamt für Verfassungsschutz	"Cyberangriff russischen Ursprungs" [Cyber attack of Russian origin, own translation]	ZEIT ONLINE, Reuters, js (2018): Maaßen spricht von Attacke russischen Ursprungs [in German only].
14-17	n.d. May 2018	Report	Bundesamt für Verfassungsschutz	"APT28" (within the chapter "Russische Cyberangriffskampagnen" [Russian cyber campaigns])	Bundesamt für Verfassungsschutz (2018): Nachrichtendienstlich gesteuerte Cyberangriffe [in German only].
			Bundesamt für Verfassungsschutz	"APT28" (within the chapter "Russische Cyberangriffskampagnen" [Russian cyber campaigns])	
			Bundesamt für Verfassungsschutz	"APT3" (within the chapter "Chinesische Cyberangriffskampagnen" [Chinese cyber campaigns])	
			Bundesamt für Verfassungsschutz	"Copy Kitten" (within the chapter "Iranische Cyberangriffskampagnen" [Iranian cyber campaigns])	
18	07 June 2018	Alert	Bundesamt für Verfassungsschutz	"APT Berserk Bear – auch Energetic Bear, Crouching Yeti oder Dragonfly genannt" [APT Berserk Bear - also called Energetic Bear, Crouching Yeti or Dragonfly, own translation]	Bundesamt für Verfassungsschutz (2018): BfV Cyber-Brief Nr. 01/2018 [in German only].
19	12 July 2018	Alert	Bundesamt für Verfassungsschutz	"APT-Gruppierung SANDWORM" [APT group Sandworm, own translation]	Bundesamt für Verfassungsschutz (2018): BfV Cyber-Brief Nr. 02/2018 [in German only].

	Day Month Year	Communication channel	Attributing actor	Attributed actor	Source
20	29 November 2018	Quote	Bundesamt für Verfassungsschutz	"im Rahmen der Bearbeitung der Cyberangriffskampagne 'Snake' [hat das BfV] aktuell erneut Angriffe detektieren können" [the BfV has been able to detect additional attacks in the context of its work on the cyber attack campaign Snake, own translation]	Spiegel (2018): Neue Hackerattacke auf Politiker, Bundeswehr und Botschaften.
				2019	
21-22	26 June 2019	Report	Bundesamt für Verfassungsschutz	"GRU für eine Welle von Cyberangriffen verantwortlich ist, die APT 28 zugeschrieben werden" [GRU is responsible for wave of cyberattacks attributed to APT 28, own translation]	Bundesministerium des Innern, für Bau und Heimat (2019): Verfassungsschutzbericht 2018 [in German only].
			Bundesamt für Verfassungsschutz	"russische[...] staatlichen Stellen" [Russian governmental entities, own translation]	
23	06 December 2019	Alert	Bundesamt für Verfassungsschutz	" WinNTI"	Bundesamt für Verfassungsschutz (2019): BfV Cyber-Brief Nr. 01/2019 [in German only].
				2020	
24	09 July 2020	Report	Bundesamt für Verfassungsschutz	"APT28"	Bundesministerium des Innern, für Bau und Heimat (2020): Verfassungsschutzbericht 2019 [in German only].
				2021	
25	15 April 2021	EU Declaration	"European Union and its Member States"	"which, the United States assesses, has been conducted by the Russian Federation"	Council of the EU (2021): Declaration by the High Representative on behalf of the European Union expressing solidarity with the United States on the impact of the SolarWinds cyber operation.
26	15 June 2021	Report	Bundesamt für Verfassungsschutz	"APT28"	Bundesministerium des Innern, für Bau und Heimat (2021): Verfassungsschutzbericht 2020 [in German only].

	Day Month Year	Communication channel	Attributing actor	Attributed actor	Source
27	19 July 2021	EU Declaration	"EU and its member states"	"undertaken from the territory of China"	Council of the EU (2021): China: Declaration by the High Representative on behalf of the European Union urging Chinese authorities to take action against malicious cyber activities undertaken from its territory.
28	06 September 2021	Press conference	Federal Foreign Office	"russischen Militärgeheimdienst GRU" [Russian military intelligence service GRU, own translation]	Auswärtiges Amt (2021): Cyberangriffe auf Bundestagsabgeordnete und Landtagsabgeordnete durch den Cyberakteur „Ghostwriter" [in German only]. Subsequent EU Declaration: Council of the EU (2021): Declaration by the High Representative on behalf of the European Union on respect for the EU's democratic processes.
			2022		
29	26 January 2022	Alert	Bundesamt für Verfassungsschutz	"APT27"	Bundesamt für Verfassungsschutz (2022): BfV Cyber-Brief Nr. 01/2022 [in German only].
30	10 May 2022	Statement	Federal Foreign Office	"Russische Föderation" [Russian Federation, own translation]	Auswärtiges Amt (2022): Auswärtiges Amt verurteilt Cyberangriff der Russischen Föderation [in German only]. Simultaneous EU Declaration: Council of the EU (2022): Russian cyber operations against Ukraine: Declaration by the High Representative on behalf of the European Union.
31	07 June 2022	Report	Bundesamt für Verfassungsschutz	"APT 28"	Bundesministerium des Innern und für Heimat (2022): Verfassungsschutzbericht 2021 [in German only].

🇩🇪	Day Month Year	Communication channel	Attributing actor	Attributed actor	Source
				2023	
32	20 March 2023	Alert	Bundesamt für Verfassungsschutz (with 🇰🇷 National Intelligence Service)	“KIMSUKY”	Bundesamt für Verfassungsschutz (2023): Warning on KIMSUKY Cyber Actor’s Recent Cyber Campaigns against Google's Browser and App Store Service.

III. Japan

OPPA Profile: Japan

Parameters	Options
Choice of communication channel	Choice of technical communication channel
	Choice of political communication channel
	Choice of criminal law or economic sanctions channel
	Combination of various communication channels as part of a coordinated attribution practice
Selection of government entity(ies) communicating the OPPA	Designation of Ministry of Foreign Affairs, national cybersecurity/intelligence/law enforcement agency, or another government entity as communicator of the OPPA
	Joint issuance of OPPA by multiple domestic authorities
Factual description of the operation attributed	Indication of (type of) target/victim and/or its location
	Indication of date when the operation attributed took place and, if applicable, its duration
	Indication of harm and/or damage caused by the operation attributed
Provision of details on the attributed actor	Reference to individuals working for organs or entities of a particular state
	Reference to organs or entities of a particular state
	Reference to actors operating under the direction of or sponsorship by a specific organ/entity of a particular state
	Reference to actors operating under the direction of or sponsorship by government of a particular state
	Reference to government of a particular state
	Reference to “state X”
	Exclusive reference to a specific APT group
	Additional provision of details about the location out of which the attributed actor has operated
	Additional inclusion of reference to prior activities/operations of attributed actor
Inclusion of a message to the attributed actor	Appeal to the attributed actor to cease activity(ies) attributed
	Announcement of possible further consequences

Parameters	Options
 Provision of or reference to evidence	Mentioning of existence or general reliance on technical evidence without further details
	Reference to governmental sources of evidence
	Reference to commercial reporting
	Provision of technical information
 Inclusion of estimative probability	Inclusion of a level of confidence or likelihood
 Engagement in international cooperation and coordination efforts	Participation in internationally coordinated attribution
	Support of OPPA practice by another state with own attribution assessment
	Support of OPPA practice by another state without own attribution assessment
	Retrospective endorsement of an OPPA by another state
	Reference to evidence of international origin or OPPAs of other states
 Specification of the severity of the operation attributed	Indication of effect and/or impact of operation attributed
	Indication of threats and/or risks posed by operation attributed
	Indication of assumed goals of attributed actor
 Formulation of policy objectives pursued with OPPA	Exposure of or response to malicious cyber activity
	Imposition of pressure, costs, or consequences
	Provision of information, awareness raising and/or warning of organizations
	Defense and protection of national interests or allies
 Linkage to national (attribution) policy	Reference to national strategies/policy documents
	Mentioning of domestic or international cybersecurity response actions
 Inclusion of reference to prior OPPAs	Inclusion of a reference to own previous OPPA practices in general or to the same attributed actor

Parameters	Options
 Reference to cyber norms or other commitments	Indirect or explicit reference to UN cyber norms or the framework of responsible state behavior
	Reference to bilateral or international commitments
	Mentioning non-compliance with a specific cyber norm or other commitments

List of Japanese OPPA Practices

	Day Month Year	Communication channel	Attributing actor	Attributed actor	Source
			2017		
1	20 December 2017	Statement	Ministry of Foreign Affairs	“North Korea”	Ministry of Foreign Affairs of Japan (2017): The U.S. Statement on North Korea’s Cyberattacks (Statement by Press Secretary Norio Maruyama).
			2018		
2-3	21 December 2018	Statement	Ministry of Foreign Affairs	“group [...] based in China known as APT10”	Ministry of Foreign Affairs of Japan (2018): Cyberattacks by a group based in China known as APT10 (Statement by Press Secretary Takeshi Osuga).
		Alert	National Center of Incident Readiness and Strategy for Cybersecurity	“APT10”	National Center of Incident Readiness and Strategy for Cybersecurity (2018): APT10 といわれるグループによるサイバー攻撃について（注意喚起) [in Japanese only].
			2019		
			2020		
			2021		
4	22 April 2021	Press conference	National Police Agency	Unit 61419 of PLA of PRC (Tick)	National Police Agency (2021): 国家公安委員会委員長記者会見要旨 [in Japanese only].
5	19 July 2021	Statement	Ministry of Foreign Affairs	“APT40 which the Chinese government is behind”	Ministry of Foreign Affairs of Japan (2021): Cases of cyberattacks including those by a group known as APT40 which the Chinese government is behind (Statement by Press Secretary YOSHIDA Tomoyuki).
			2022		
6	14 October 2022	Alert	National Police Agency, Financial Services Agency & National Center of Incident Readiness and Strategy for Cybersecurity	Lazarus Group, DPRK authorities	National Police Agency, Financial Services Agency & National Center of Incident Readiness and Strategy for Cybersecurity (2022): 北朝鮮当局の下部組織とされるラザルスと呼称されるサイバー攻撃グループによる暗号資産関連事業者等を標的としたサイバー攻撃について（注意喚起) [in Japanese only]

IV. United States of America

OPPA Profile: U.S.

Parameters	Options
 Choice of communication channel	Choice of technical communication channel
	Choice of political communication channel
	Choice of criminal law or economic sanctions channel
	Combination of various communication channels as part of a coordinated attribution practice
 Selection of government entity(ies) communicating the OPPA	Designation of Ministry of Foreign Affairs, national cybersecurity/intelligence/law enforcement agency, or another government entity as communicator of the OPPA
	Joint issuance of OPPA by multiple domestic authorities
 Factual description of the operation attributed	Indication of (type of) target/victim and/or its location
	Indication of date when the operation attributed took place and, if applicable, its duration
	Indication of harm and/or damage caused by the operation attributed
 Provision of details on the attributed actor	Reference to individuals working for organs or entities of a particular state
	Reference to organs or entities of a particular state
	Reference to actors operating under the direction of or sponsorship by a specific organ/entity of a particular state
	Reference to actors operating under the direction of or sponsorship by government of a particular state
	Reference to government of a particular state
	Reference to “state X”
	Exclusive reference to a specific APT group
	Additional provision of details about the location out of which the attributed actor has operated
	Additional inclusion of reference to prior activities/operations of attributed actor
 Inclusion of a message to the attributed actor	Appeal to the attributed actor to cease activity(ies) attributed
	Announcement of possible further consequences

Parameters	Options
 Provision of or reference to evidence	Mentioning of existence or general reliance on technical evidence without further details
	Reference to governmental sources of evidence
	Reference to commercial reporting
	Provision of technical information
 Inclusion of estimative probability	Inclusion of a level of confidence or likelihood
 Engagement in international cooperation and coordination efforts	Participation in internationally coordinated attribution
	Support of OPPA practice by another state with own attribution assessment
	Support of OPPA practice by another state without own attribution assessment
	Retrospective endorsement of an OPPA by another state
	Reference to evidence of international origin or OPPAs of other states
 Specification of the severity of the operation attributed	Indication of effect and/or impact of operation attributed
	Indication of threats and/or risks posed by operation attributed
	Indication of assumed goals of attributed actor
 Formulation of policy objectives pursued with OPPA	Exposure of or response to malicious cyber activity
	Imposition of pressure, costs, or consequences
	Provision of information, awareness raising and/or warning of organizations
	Defense and protection of national interests or allies
 Linkage to national (attribution) policy	Reference to national strategies/policy documents
	Mentioning of domestic or international cybersecurity response actions
 Inclusion of reference to prior OPPAs	Inclusion of a reference to own previous OPPA practices in general or to the same attributed actor

Parameters	Options
 Reference to cyber norms or other commitments	Indirect or explicit reference to UN cyber norms or the framework of responsible state behavior
	Reference to bilateral or international commitments
	Mentioning non-compliance with a specific cyber norm or other commitments

List of U.S. OPPA Practices

	Day Month Year	Communication channel	Attributing actor	Attributed actor	Source
				2014	
1	19 May 2014	Indictment	DOJ	"Wang Dong, Sun Kailiang, Wen Xinyu, Huang Zhenyu, and Gu Chunhui, who were officers in Unit 61398 of the Third Department of the Chinese People's Liberation Army (PLA)"	Department of Justice (2014): U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage.
2	19 December 2014	Statement	FBI	"North Korean government"	Federal Bureau of Investigation (2014): Update on Sony Investigation.
				2015	
3	26 February 2015	Statement	Director of National Intelligence	"2014 saw [...] cyberattacks carried out on U.S. soil by nation-state entities [for example] the Iranian attack"	United States Senate (2015): Committee on Armed Services, Hearing to Receive Testimony on Worldwide Threats, Thursday, February 26, 2015.
				2016	
4	24 March 2016	Indictment	DOJ	"seven Iranian individuals who were employed by two Iran-based computer companies, ITSecTeam (ITSEC) and Mersad Company (MERSAD), that performed work on behalf of the Iranian Government, including the Islamic Revolutionary Guard Corps"	Department of Justice (2016): Seven Iranians Working for Islamic Revolutionary Guard Corps-Affiliated Entities Charged for Conducting Coordinated Campaign of Cyber Attacks Against U.S. Financial Sector.
5	7 October 2016	Statement	DHS & Office of the Director of National Intelligence	"Russian Government"	Department of Homeland Security and Director of National Intelligence (2017): Joint Statement from the Department Of Homeland Security and Office of the Director of National Intelligence on Election Security.
6	29 December 2016	Report	DHS & FBI	"Russian civilian and military intelligence Services"	NCCIC and Federal Bureau of Investigation (2016): GRIZZLY STEPPE – Russian Malicious Cyber Activity.
				2017	
7	15 March 2017	Indictment	DOJ	"four defendants, including two officers of the Russian Federal Security Service (FSB)"	Department of Justice (2017): U.S. Charges Russian FSB Officers and Their Criminal Conspirators for Hacking Yahoo and Millions of Email Accounts.

	Day Month Year	Communication channel	Attributing actor	Attributed actor	Source
8	13 June 2017	Alert	DHS & FBI	"cyber actors of the North Korean government"	Department of Homeland Security and Federal Bureau of Investigation (2017): HIDDEN COBRA – North Korea's DDoS Botnet Infrastructure.
9	14 November 2017	Alert	DHS & FBI	"North Korean government"	Department of Homeland Security and Federal Bureau of Investigation (2017): HIDDEN COBRA – North Korean Remote Administration Tool: FALLCHILL.
10	14 November 2017	Alert	DHS & FBI	"North Korean government"	Department of Homeland Security and Federal Bureau of Investigation (2017): HIDDEN COBRA – North Korean Trojan: Volgmer.
11	19 December 2017	Press conference	United States Homeland Security Advisor	"North Korea"	The White House (2017): Press Briefing on the Attribution of the WannaCry Malware Attack to North Korea.
				2018	
12	15 February 2018	Press statement	White House Press Secretary	"Russian military"	The White House (2018): Statement from the Press Secretary.
13	15 March 2018	Alert	DHS & FBI	"Russian government cyber actors"	Department of Homeland Security and Federal Bureau of Investigation (2018): Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors.
14	23 March 2018	Indictment	DOJ	"defendants conducted many of these intrusions on behalf of the Islamic Republic of Iran's (Iran) Islamic Revolutionary Guard Corps (IRGC)"	Department of Justice (2018): Nine Iranians Charged With Conducting Massive Cyber Theft Campaign on Behalf of the Islamic Revolutionary Guard Corps.
15	16 April 2018	Alert	DHS & FBI (with NCSC)	"Russian state-sponsored cyber actors"	Department of Homeland Security, Federal Bureau of Investigation and United Kingdom's National Cyber Security Centre (2018): Russian State-Sponsored Cyber Actors Targeting Network Infrastructure Devices.
16	29 May 2018	Alert	DHS & FBI	"North Korean government"	Department of Homeland Security and Federal Bureau of Investigation (2018): HIDDEN COBRA – Joanap Backdoor Trojan and Brambul Server Message Block Worm.
17	14 June 2018	Report	DHS & FBI	"North Korean government"	Department of Homeland Security and Federal Bureau of Investigation (2018): MAR-10135536-12 – North Korean Trojan: TYPEFRAME.

	Day Month Year	Communication channel	Attributing actor	Attributed actor	Source
18	13 July 2018	Indictment	DOJ	"all twelve defendants are members of the GRU, a Russian Federation intelligence agency within the Main Intelligence Directorate of the Russian military"	Department of Justice (2018): Grand Jury Indicts 12 Russian Intelligence Officers for Hacking Offenses Related to the 2016 Election.
19	9 August 2018	Report	DHS & FBI	"North Korean government"	Department of Homeland Security and Federal Bureau of Investigation (2018): MAR-10135536-17 – North Korean Trojan: KEYMARBLE.
20-21	6 September 2018	Indictment	DOJ	"North Korean Regime-Backed Programmer"	Department of Justice (2018): North Korean Regime-Backed Programmer Charged With Conspiracy to Conduct Multiple Cyber Attacks and Intrusions.
		Sanction	Department of the Treasury's Office of Foreign Assets Control	"one entity and one individual tied to the Government of North Korea's malign cyber activities"	Department of the Treasury (2018): Treasury Targets North Korea for Multiple Cyber-Attacks.
22	2 October 2018	Alert	DHS, Department of the Treasury & FBI	"North Korean government"	Department of Homeland Security, Department of the Treasury, and Federal Bureau of Investigation (2018): HIDDEN COBRA – FASTCash Campaign.
23	4 October 2018	Indictment	DOJ	"seven defendants, all officers in the Russian Main Intelligence Directorate (GRU), a military intelligence agency of the General Staff of the Armed Forces of the Russian Federation"	Department of Justice (2018): U.S. Charges Russian GRU Officers with International Hacking and Related Influence and Disinformation Operations.
24	30 October 2018	Indictment	DOJ	"charged intelligence officers, Zha Rong and Chai Meng, and other co-conspirators, worked for the Jiangsu Province Ministry of State Security ("JSSD"), headquartered in Nanjing, which is a provincial foreign intelligence arm of the People's Republic of China's Ministry of State Security ("MSS")"	Department of Justice (2018): Chinese Intelligence Officers and Their Recruited Hackers and Insiders Conspired to Steal Sensitive Commercial Aviation and Technological Data for Years.

	Day Month Year	Communication channel	Attributing actor	Attributed actor	Source
25-26	20 December 2018	Indictment	DOJ	"Members of the APT 10 Hacking Group Who Acted in Association with the Tianjin State Security Bureau"	Department of Justice (2018): Two Chinese Hackers Associated With the Ministry of State Security Charged with Global Computer Intrusion Campaigns Targeting Intellectual Property and Confidential Business Information.
		Statement	Secretary of State and Secretary of Homeland Security	"Chinese cyber actors associated with the Chinese Ministry of State Security"	Department of State (2018): Joint Statement by Secretary of State Michael R. Pompeo and Secretary of Homeland Security Kirstjen Nielsen: Chinese Actors Compromise Global Managed Service Providers.
				2019	
27	13 February 2019	Indictment	DOJ	"Cyber Conspirators [...] working on behalf of the Iranian Revolutionary Guard Corps"	Department of Justice (2019): Former U.S. Counterintelligence Agent Charged With Espionage on Behalf of Iran; Four Iranians Charged With a Cyber Campaign Targeting Her Former Colleagues.
28	9 September 2019	Report	DHS, FBI, DoD	"North Korean government"	Department of Homeland Security, Federal Bureau of Investigation, and Department of Defense (2019): MAR-10135536-21 – North Korean Proxy Malware: ELECTRICFISH.
29	9 September 2019	Report	DHS, FBI, DoD	"North Korean government"	Department of Homeland Security, Federal Bureau of Investigation, and Department of Defense (2019): MAR-10135536-10 – North Korean Trojan: BADCALL.
				2020	
30	10 February 2020	Indictment	DOJ	"Four Members of China's People's Liberation Army"	Department of Justice (2020): Chinese Military Personnel Charged with Computer Fraud, Economic Espionage and Wire Fraud for Hacking into Credit Reporting Agency Equifax.
31	14 February 2020	Report	DHS, FBI, DoD	"North Korean government"	Department of Homeland Security, Federal Bureau of Investigation, and Department of Defense (2020): MAR-10265965-1.v1 – North Korean Trojan: BISTROMATH.
32	14 February 2020	Report	DHS, FBI, DoD	"North Korean government"	Department of Homeland Security, Federal Bureau of Investigation, and Department of Defense (2020): MAR-10265965-2.v1 – North Korean Trojan: SLICKSHOES.

	Day Month Year	Communication channel	Attributing actor	Attributed actor	Source
33	14 February 2020	Report	DHS, FBI, DoD	"North Korean government"	Department of Homeland Security, Federal Bureau of Investigation, and Department of Defense (2020): MAR-10265965-3.v1 – North Korean Trojan: CROWDEDFLOUNDER.
34	14 February 2020	Report	DHS, FBI, DoD	"North Korean government"	Department of Homeland Security, Federal Bureau of Investigation, and Department of Defense (2020): MAR-10271944-1.v1 – North Korean Trojan: HOTCROISSANT.
35	14 February 2020	Report	DHS, FBI, DoD	"North Korean government"	Department of Homeland Security, Federal Bureau of Investigation, and Department of Defense (2020): MAR-10271944-2.v1 – North Korean Trojan: ARTFULPIE.
36	14 February 2020	Report	DHS, FBI, DoD	"North Korean government"	Department of Homeland Security, Federal Bureau of Investigation, and Department of Defense (2020): MAR-10271944-3.v1 – North Korean Trojan: BUFFETLINE.
37	14 February 2020	Report	DHS, FBI, DoD	"North Korean government"	Department of Homeland Security, Federal Bureau of Investigation, and Department of Defense (2020): MAR-10135536-8.v4 – North Korean Trojan: HOPLIGHT.
38	20 February 2020	Statement	Secretary of State	"Russian General Staff Main Intelligence Directorate (GRU) Main Center for Special Technologies (GTsST, also known as Unit 74455 and Sandworm)"	Department of State (2020): The United States Condemns Russian Cyber Attack Against the Country of Georgia.
39-40	15 April 2020	Advisory	State Department, DHS, Treasury Department, FBI	"DPRK"	Departments of State, the Treasury, and Homeland Security, and Federal Bureau of Investigation (2020): Guidance on the North Korean Cyber Threat.
		Statement	State Department	"North Korea"	Department of State (2020): The United States Issues an Advisory on North Korean Cyber Threats.

	Day Month Year	Communication channel	Attributing actor	Attributed actor	Source
41	12 May 2020	Report	DHS, FBI, DoD	"North Korean government"	Department of Homeland Security, Federal Bureau of Investigation, and Department of Defense (2020): MAR-10288834-1.v1 – North Korean Remote Access Tool: COPPERHEDGE.
42	12 May 2020	Report	DHS, FBI, DoD	"North Korean government"	Department of Homeland Security, Federal Bureau of Investigation, and Department of Defense (2020): MAR-10288834-2.v1 – North Korean Trojan: TAINTEDSCRIBE.
43	12 May 2020	Report	DHS, FBI, DoD	"North Korean government"	Department of Homeland Security, Federal Bureau of Investigation, and Department of Defense (2020): MAR-10288834-3.v1 – North Korean Trojan: PEBBLEDASH.
44-45	13 May 2020	Statement	FBI, CISA	"PRC-affiliated cyber actors"	Federal Bureau of Investigation and Cybersecurity and Infrastructure Security Agency (2020): FBI-CISA PSA PRC Targeting of COVID-19 Research Organizations.
		Statement	Secretary of State	"cyber actors and non-traditional collectors affiliated with the People's Republic of China"	Department of State (2020): The United States Condemns Attempts by P.R.C.-Affiliated Actors To Steal American COVID-19 Research.
46	28 May 2020	Advisory	NSA	"Russian cyber actors from the GRU Main Center for Special Technologies (GTsST), field post number 74455"	National Security Agency (2020): Sandworm Actors Exploiting Vulnerability in Exim Mail Transfer Agent.
47	21 July 2020	Indictment	DOJ	"Two Chinese Hackers Working with the Ministry of State Security"	Department of Justice (2020): Two Chinese Hackers Working with the Ministry of State Security Charged with Global Computer Intrusion Campaign Targeting Intellectual Property and Confidential Business Information, Including COVID-19 Research.
48	3 August 2020	Report	CISA, FBI, DoD	"Chinese government actors"	Cybersecurity and Infrastructure Security Agency, Federal Bureau of Investigation and Department of Defense (2020): MAR-10292089-1.v2 – Chinese Remote Access Trojan: TAIDOOR.
49	13 August 2020	Advisory	NSA, FBI	"Russian General Staff Main Intelligence Directorate (GRU) 85th Main Special Service Center (GTsSS), military unit 26165"	National Security Agency and Federal Bureau of Investigation (2020): Russian GRU 85th GTsSS Deploys Previously Undisclosed Drovorub Malware.

	Day Month Year	Communication channel	Attributing actor	Attributed actor	Source
50	19 August 2020	Report	CISA, FBI	"North Korean government"	Federal Bureau of Investigation and Cybersecurity and Infrastructure Security Agency (2020): MAR-10295134-1.v1 – North Korean Remote Access Trojan: BLINDINGCAN.
51	26 August 2020	Advisory	CISA, Department of Treasury, FBI, U.S. Cyber Command	"North Korean government"	Cybersecurity and Infrastructure Security Agency, Department of the Treasury, Federal Bureau of Investigation and U.S. Cyber Command (2020): FASTCash 2.0: North Korea's BeagleBoyz Robbing Banks.
52	14 September 2020	Advisory	CISA	"Chinese Ministry of State Security (MSS)-affiliated cyber threat actors"	Cybersecurity and Infrastructure Security Agency (2020): Chinese Ministry of State Security-Affiliated Cyber Threat Actor Activity.
53	16 September 2020	Indictment	DOJ	"Apt41" Actors"	Department of Justice (2020): Seven International Cyber Defendants, Including "Apt41" Actors, Charged In Connection With Computer Intrusion Campaigns Against More Than 100 Victims Globally.
54	16 September 2020	Indictment	DOJ	"Two Iranian nationals have been charged in connection with a coordinated cyber intrusion campaign – sometimes at the behest of the government of the Islamic Republic of Iran"	Department of Justice (2020): Two Iranian Nationals Charged in Cyber Theft Campaign Targeting Computer Systems in United States, Europe, and the Middle East.
55-57	17 September 2020	Sanction	Department of the Treasury's Office of Foreign Assets Control	"Iranian cyber threat group Advanced Persistent Threat 39 (APT39), 45 associated individuals, and one front company. Masked behind its front company, Rana Intelligence Computing Company (Rana), the Government of Iran (GOI) ..."	Department of the Treasury (2020): Treasury Sanctions Cyber Actors Backed by Iranian Intelligence Ministry.
		Statement	Secretary of State	"Cyber Actors Backed by Iranian Intelligence Ministry"	Department of State (2020): The United States Sanctions Cyber Actors Backed by Iranian Intelligence Ministry.
		Advisory	FBI	"Iranian nation state actors publicly known as Advanced Persistent Threat 39 [...] masked behind its front company, Rana Intelligence Computing Company (Rana), the Government of Iran's Ministry of Intelligence and Security"	Federal Bureau of Investigation (2020): FBI Releases Cybersecurity Advisory on Previously Undisclosed Iranian Malware Used to Monitor Dissidents and Travel and Telecommunications Companies.

	Day Month Year	Communication channel	Attributing actor	Attributed actor	Source
58	17 September 2020	Indictment	DOJ	"three computer hackers [...] engaging in a coordinated campaign of identity theft and hacking on behalf of Iran's Islamic Revolutionary Guard Corps"	Department of Justice (2020): State-Sponsored Iranian Hackers Indicted for Computer Intrusions at U.S. Satellite Companies.
59	1 October 2020	Alert	CISA	"Chinese government and affiliated cyber threat actor"	Cybersecurity and Infrastructure Security Agency (2020): Potential for China Cyber Response to Heightened U.S.–China Tensions.
60	20 October 2020	Advisory	NSA	"Chinese state-sponsored cyber actors"	National Security Agency (2020): Chinese State-Sponsored Actors Exploit Publicly Known Vulnerabilities.
61-62	19 October 2020	Indictment	DOJ	"six [...] officers in Unit 74455 of the Russian Main Intelligence Directorate"	Department of Justice (2020): Six Russian GRU Officers Charged in Connection with Worldwide Deployment of Destructive Malware and Other Disruptive Actions in Cyberspace.
		Statement	Secretary of State	"six officers of the Russian General Staff Main Intelligence Directorate's (GRU) Military Unit 74455"	Department of State (2020): United States Charges Russian Military Intelligence Officers for Cyber Crimes.
63	22 October 2020	Advisory	FBI, CISA	"Russian state-sponsored APT actor—known variously as Berserk Bear, Energetic Bear, TeamSpy, Dragonfly, Havex, Crouching Yeti, and Koala in open-source reporting"	Federal Bureau of Investigation and Cybersecurity and Infrastructure Security Agency (2020): Russian State-Sponsored Advanced Persistent Threat Actor Compromises U.S. Government Targets.
64	22 October 2020	Advisory	FBI, CISA	"Iranian State-Sponsored Advanced Persistent Threat Actors"	Federal Bureau of Investigation and Cybersecurity and Infrastructure Security Agency (2020): Iranian State-Sponsored Advanced Persistent Threat Actors Threaten Election-Related Systems.

	Day Month Year	Communication channel	Attributing actor	Attributed actor	Source
65-66	23 October 2020	Sanction	Department of the Treasury's Office of Foreign Assets Control	"tate Research Center of the Russian Federation FGUP Central Scientific Research Institute of Chemistry and Mechanics (TsNIIKhM), a Russian government-controlled research institution"	Department of the Treasury (2020): Treasury Sanctions Russian Government Research Institution Connected to the Triton Malware.
		Statement	Secretary of State	"State Research Center of the Russian Federation FGUP Central Scientific Research Institute of Chemistry and Mechanics (TsNIIKhM), a Russian government-controlled research institution"	Department of State (2020): United States Sanctions Russian Government Research Institution.
67	27 October 2020	Advisory	CISA, FBI, U.S. Cyber Command Cyber National Mission Force	"North Korean advanced persistent threat (APT) group Kimsuky [...] North Korean government"	Cybersecurity and Infrastructure Security Agency, Federal Bureau of Investigation and U.S. Cyber Command Cyber National Mission Force (2020): North Korean Advanced Persistent Threat Focus: Kimsuky.
68	30 October 2020	Advisory	CISA, FBI	"Iranian advanced persistent threat (APT) actor"	Federal Bureau of Investigation and Cybersecurity and Infrastructure Security Agency (2020): Iranian Advanced Persistent Threat Actor Identified Obtaining Voter Registration Data.
				2021	
69	5 January 2021	Statement	FBI, CISA, ODNI, NSA	"Advanced Persistent Threat (APT) actor, likely Russian in origin, [...] we believe this was, and continues to be, an intelligence gathering effort."	Federal Bureau of Investigation, FBICybersecurity and Infrastructure Security Agency, Office of the Director of National Intelligence and National Security Agency (2021): Joint Statement by the Federal Bureau of Investigation (FBI), the Cybersecurity and Infrastructure Security Agency (CISA), the Office of the Director of National Intelligence (ODNI), and the National Security Agency (NSA).
70-71	17 February 2021	Indictment	DOJ	"members of units of the Reconnaissance General Bureau"	Department of Justice (2021): Three North Korean Military Hackers Indicted in Wide-Ranging Scheme to Commit Cyberattacks and Financial Crimes Across the Globe.
		Advisory	FBI, CISA, Treasury	"Lazarus Group—which these agencies attribute to North Korean state-sponsored advanced persistent threat (APT) actors"	Federal Bureau of Investigation, Cybersecurity and Infrastructure Security Agency, and Department of the Treasury (2020): AppleJeus: Analysis of North Korea's Cryptocurrency Malware.

	Day Month Year	Communication channel	Attributing actor	Attributed actor	Source
72-75	15 April 2021	Statement	White House	"Russian Foreign Intelligence Service (SVR), also known as APT 29, Cozy Bear, and The Dukes"	The White House (2021): Fact Sheet: Imposing Costs for Harmful Foreign Activities by the Russian Government.
		Statement	Secretary of State	"Russian Government"	Department of State (2021): Holding Russia To Account.
		Advisory	NSA, CISA, FBI	"Russian Foreign Intelligence Service (SVR) actors (also known as APT29, Cozy Bear, and The Dukes)"	National Security Agency, Federal Bureau of Investigation and Cybersecurity and Infrastructure Security Agency (2021): Russian SVR Targets U.S. and Allied Networks.
		Sanction	Treasury	"companies operating in the technology sector of the Russian Federation economy that support Russian Intelligence Services [...] supports units of Russia's Main Intelligence Directorate (GRU) responsible for offensive cyber and information operations [... inter alia] SVA is a Russian state-owned research institute specializing in advanced systems for information security located in Russia. SVA conducted research and development in support of the SVR's malicious cyber operations. [...]"	Department of the Treasury (2021): Treasury Sanctions Russia with Sweeping New Sanctions Authority.
76	26 April 2021	Advisory	FBI, CISA, DHS	"Russian Foreign Intelligence Service (SVR) cyber actors—also known as Advanced Persistent Threat 29 (APT 29), the Dukes, CozyBear, and Yttrium"	Federal Bureau of Investigation, Cybersecurity and Infrastructure Security Agency and Department of Homeland Security (2021): Russian Foreign Intelligence Service (SVR) Cyber Operations: Trends and Best Practices for Network Defenders.
77	1 July 2021	Advisory	NSA, CISA, FBI (with NCSC)	"Russian General Staff Main Intelligence Directorate (GRU) 85th Main Special Service Center (GTsSS), military unit 26165"	National Security Agency, Cybersecurity and Infrastructure Security Agency, Federal Bureau of Investigation et al. (2021): Russian GRU Conducting Global Brute Force Campaign to Compromise Enterprise and Cloud Environments.
78	16 July 2021	Advisory	NSA, CISA (with NCSC, CSE)	"APT29 (also known as 'the Dukes' or 'Cozy Bear') is a cyber espionage group, almost certainly part of the Russian intelligence services"	National Security Agency, Cybersecurity and Infrastructure Security Agency et al. (2021): Advisory: APT29 targets COVID-19 vaccine development.

	Day Month Year	Communication channel	Attributing actor	Attributed actor	Source
79	19 July 2021	Advisory	FBI, CISA	"Indicted APT40 Actors Associated with China's MSS Hainan State Security Department"	Federal Bureau of Investigation and Cybersecurity and Infrastructure Security Agency (2021): Tactics, Techniques, and Procedures of Indicted APT40 Actors Associated with China's MSS Hainan State Security Department.
80-83	19 July 2021	Statement	White House	"MSS-affiliated cyber operators"	The White House (2021): The United States, Joined by Allies and Partners, Attributes Malicious Cyber Activity and Irresponsible State Behavior to the People's Republic of China.
		Statement	Secretary of State	"cyber actors affiliated with the MSS"	Department of State (2021): Responding to the PRC's Destabilizing and Irresponsible Behavior in Cyberspace.
		Advisory	CISA, FBI	"Chinese state-sponsored cyber actors"	Federal Bureau of Investigation and Cybersecurity and Infrastructure Security Agency (2021): Chinese State-Sponsored Cyber Operations: Observed TTPs.
		Indictment	DOJ	"Officers in the Hainan State Security Department (HSSD), a provincial arm of China's Ministry of State Security (MSS)"	Department of Justice (2021): Four Chinese Nationals Working with the Ministry of State Security Charged with Global Computer Intrusion Campaign Targeting Intellectual Property and Confidential Business Information, Including Infectious Disease Research.
84	20 July 2021	Advisory	CISA, FBI	"state-sponsored Chinese actors"	Federal Bureau of Investigation and Cybersecurity and Infrastructure Security Agency (2021): Chinese Gas Pipeline Intrusion Campaign, 2011 to 2013.
85	17 November 2021	Advisory	FBI, CISA (with ACSC, NCSC)	"Iranian Government-Sponsored APT Cyber Actors"	Federal Bureau of Investigation, Cybersecurity and Infrastructure Security Agency et al. (2021): Iranian Government-Sponsored APT Cyber Actors Exploiting Microsoft Exchange and Fortinet Vulnerabilities in Furtherance of Malicious Activities.

	Day Month Year	Communication channel	Attributing actor	Attributed actor	Source
86-87	18 November 2021	Indictment	DOJ	"Kazemi and Kashian [...] worked as contractors for an Iran-based company formerly known as Eeleyanet Gostar [...] Among other things, Eeleyanet Gostar is known to have provided services to the Iranian government, including to the Guardian Council."	Department of Justice (2021): Two Iranian Nationals Charged for Cyber-Enabled Disinformation and Threat Campaign Designed to Influence the 2020 U.S. Presidential Election.
		Statement	Secretary of State	"State-sponsored actors, including Iranian groups"	Department of State (2021): Designation of Iranian Cyber Actors for Attempting to Influence the 2020 U.S. Presidential Election.
				2022	
88	16 February 2022	Advisory	FBI, NSA, CISA	"Russian state-sponsored cyber actors"	Federal Bureau of Investigation, National Security Agency and Cybersecurity and Infrastructure Security Agency (2022): Russian State-Sponsored Cyber Actors Target Cleared Defense Contractor Networks to Obtain Sensitive U.S. Defense Information and Technology.
89	18 February 2022	Press conference	White House	"Russian Main Intelligence Directorate"	The White House (2022): Press Briefing by Press Secretary Jen Psaki, Deputy National Security Advisor for Cyber and Emerging Technology Anne Neuberger, and Deputy National Security Advisor for International Economics and Deputy NEC Director Daleep Singh, February 18, 2022.
90	23 February 2022	Advisory	CISA, NSA, FBI (with NCSC)	"attributed the Sandworm actor to the Russian General Staff Main Intelligence Directorate's Russian (GRU's) Main Centre for Special Technologies (GTsST)"	Cybersecurity and Infrastructure Security Agency, National Security Agency and Federal Bureau of Investigation (2022): New Sandworm Malware Cyclops Blink Replaces VPNFilter.
91	24 February 2022	Advisory	FBI, CISA, U.S. Cyber Command Cyber National Mission Force (with NCSC)	"group of Iranian government-sponsored advanced persistent threat (APT) actors, known as MuddyWater"	Federal Bureau of Investigation, Cybersecurity and Infrastructure Security Agency et al. (2022): Iranian Government-Sponsored Actors Conduct Cyber Operations Against Global Government and Commercial Networks.
92	15 March 2022	Advisory	FBI, CISA	"Russian state-sponsored cyber actors"	Federal Bureau of Investigation and Cybersecurity and Infrastructure Security Agency (2022): Russian State-Sponsored Cyber Actors Gain Network Access by Exploiting Default Multifactor Authentication Protocols and "PrintNightmare" Vulnerability.

	Day Month Year	Communication channel	Attributing actor	Attributed actor	Source
93-94	24 March 2022	Indictment	DOJ	"an employee of a Russian Ministry of Defense research institute [...] three officers of Russia's Federal Security Service (FSB)"	Department of Justice (2022): Four Russian Government Employees Charged in Two Historical Hacking Campaigns Targeting Critical Infrastructure Worldwide.
		Advisory	CISA, FBI, Department of Energy	"state-sponsored Russian cyber actors"	Cybersecurity and Infrastructure Security Agency, Federal Bureau of Investigation and Department of Energy (2022): Tactics, Techniques, and Procedures of Indicted State-Sponsored Russian Cyber Actors Targeting the Energy Sector.
95	18 April 2022	Advisory	FBI, CISA, Treasury	"North Korean state-sponsored advanced persistent threat (APT) group [...] commonly tracked by the cybersecurity industry as Lazarus Group, APT38, BlueNoroff, and Stardust Chollima"	Federal Bureau of Investigation, Cybersecurity and Infrastructure Security Agency and Department of the Treasury (2022): TraderTraitor: North Korean State-Sponsored APT Targets Blockchain Companies.
96	20 April 2022	Advisory	CISA, FBI, NSA (with ACSC, CCCS, NCSC, and NCSC and NCA)	"Russian government"	Cybersecurity and Infrastructure Security Agency, Federal Bureau of Investigation, National Security Agency et al. (2022): Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure.
97	10 May 2022	Statement	Secretary of State	"Russia"	Department of State (2022): Attribution of Russia's Malicious Cyber Activity Against Ukraine.
98	7 June 2022	Advisory	NSA, CISA, FBI	"People's Republic of China (PRC) state-sponsored cyber actors"	Cybersecurity and Infrastructure Security Agency, Federal Bureau of Investigation, and National Security Agency (2022): People's Republic of China State-Sponsored Cyber Actors Exploit Network Providers and Devices.
99	6 July 2022	Advisory	FBI, CISA, Treasury	"North Korean state-sponsored cyber actors"	Federal Bureau of Investigation, Cybersecurity and Infrastructure Security Agency and Department of the Treasury (2022): North Korean State-Sponsored Cyber Actors Use Maui Ransomware to Target the Healthcare and Public Health Sector.
100	7 September 2022	Statement	White House	"Government of Iran"	The White House (2022): Statement by NSC Spokesperson Adrienne Watson on Iran's Cyberattack against Albania.

	Day Month Year	Communication channel	Attributing actor	Attributed actor	Source
101-102	9 September 2022	Sanction	Department of the Treasury's Office of Foreign Assets Control	"Iran's Ministry of Intelligence and Security (MOIS) and its Minister of Intelligence"	Department of the Treasury (2022): Treasury Sanctions Iranian Ministry of Intelligence and Minister for Malign Cyber Activities.
		Statement	Secretary of State	"Iran's Ministry of Intelligence and Security (MOIS) and its Minister of Intelligence"	Department of State (2022): Sanctioning Iran's Ministry of Intelligence and Security for Malign Cyber Activities.
103-105	14 September 2022	Sanction	Department of the Treasury's Office of Foreign Assets Control	"IRGC-affiliated group"	Department of the Treasury (2022): Treasury Sanctions IRGC-Affiliated Cyber Actors for Roles in Ransomware Activity.
		Statement	Secretary of State	"ten individuals and two entities, all affiliated with Iran's Islamic Revolutionary Guard Corps"	Department of State (2022): Sanctioning Iranians for Malicious Cyber Acts.
		Advisory	FBI, CISA, NSA, U.S. Cyber Command, Department of the Treasury (with ACSC, CCCS, and NCSC)	"Iranian Islamic Revolutionary Guard Corps-Affiliated Cyber Actors"	Federal Bureau of Investigation, Cybersecurity and Infrastructure Security Agency, National Security Agency et al. (2022): Iranian Islamic Revolutionary Guard Corps-Affiliated Cyber Actors Exploiting Vulnerabilities for Data Extortion and Disk Encryption for Ransom Operations.
106	16 November 2022	Advisory	CISA, FBI	"Iranian government-sponsored actors"	Cybersecurity and Infrastructure Security Agency and Federal Bureau of Investigation (2022): Iranian Government-Sponsored APT Actors Compromise Federal Network, Deploy Crypto Miner, Credential Harvester.
			2023		
107	9 February 2023	Advisory	NSA, FBI, U.S. Department of Health and Human Services (with National Intelligence Service Defense Security Agency (DSA)	"DPRK cyber actors"	National Security Agency, Federal Bureau of Investigation, Cybersecurity and Infrastructure Security Agency et al. (2023): #StopRansomware: Ransomware Attacks on Critical Infrastructure Fund DPRK Malicious Cyber Activities.
108	18 April 2023	Advisory	CISA, FBI, NSA (with NCSC)	APT28	Cybersecurity and Infrastructure Security Agency, Federal Bureau of Investigation and National Security Agency et al. (2023): APT28 Exploits Known Vulnerability to Carry Out Reconnaissance and Deploy Malware on Cisco Routers.

	Day Month Year	Communication channel	Attributing actor	Attributed actor	Source
109	09 May 2023	Advisory	FBI, NSA, CISA, Cyber National Mission Force (with ACSC, NCSC, CCCS and CSE, and NCSC)	“Center 16 of Russia’s Federal Security Service (FSB)”	Federal Bureau of Investigation, National Security Agency, Cybersecurity and Infrastructure Security Agency et al. (2023): Hunting Russian Intelligence “Snake” Malware.

V. Overview: International Coordination of Focus Countries' OPPA Practices

The following table provides an overview of the focus countries' OPPA practice involving international cooperation or coordination. Where such coordination was predominantly practiced via technical channels, the respective 'operation attributed' row is colored in light orange. The respective row is white when the international coordination was pursued primarily in the form of political channels. The table includes columns for each of the four focus countries, which list both date and communication channel of the respective OPPA practice.

Operation attributed				
WannaCry	December 20, 2017: **Statement**	No OPPA	December 20, 2017: **Statement**	December 19, 2017: **Press briefing**
NotPetya	February 16, 2018: **Statement**	No OPPA[1]	No OPPA	February 15, 2018: **Press statement**
Routers	April 17, 2018: **Statement** & **Alert**[2]	June 26, 2019: **Report**	No OPPA	April 16, 2018: **Alert**[3]
DNC Hack	October 4, 2018: **Statement**[4]	June 26, 2019: **Report**	No OPPA	October 7, 2016: **Statement**
BadRabbit & TV Station	October 4, 2018: **Statement**[5]	No OPPA	No OPPA	No OPPA
WADA	October 4, 2018: **Statement**[6]	June 26, 2019: **Report**	No OPPA	October 4, 2018: **Indictment**

1 Conclusions of the Council of the EU mentioned WannaCry and NotPetya, but did not include an attribution (Council of the European Union (2018): Council conclusions on malicious cyber activities - approval).
2 Australia issued a national alert and did not participate in the U.S.-United Kingdom joint alert.
3 Together with the United Kingdom.
4 Together with the United Kingdom (National Cyber Security Centre (2018): Reckless campaign of cyber attacks by Russian military intelligence service exposed).
5 Together with the United Kingdom (National Cyber Security Centre (2018): Reckless campaign of cyber attacks by Russian military intelligence service exposed).
6 Together with the United Kingdom (National Cyber Security Centre (2018): Reckless campaign of cyber attacks by Russian military intelligence service exposed) and in coordination with the U.S. indictment.

Operation attributed	🇦🇺	🇩🇪	🇯🇵	🇺🇸
OPCW	October 5, 2018: **Statement**[7]	No OPPA[8]	No OPPA	October 4, 2018: **Indictment**
CloudHopper	December 21, 2018: **Statement**	No OPPA[9]	December 21, 2018: **Statement**	December 20, 2018: **Statement** & **Indictment**
Georgia	February 21, 2020: **Statement**	No OPPA[10]	No OPPA	February 20, 2020: **Statement**
SolarWinds	April 15, 2021: **Statement**	April 15, 2021: **EU Declaration**	No OPPA	April 15, 2021: **WH Statement** & **Advisory** & **Sanctions** & **State Statement**
COVID-19 Vaccine Development	July 17, 2020: **Statement**	No OPPA	No OPPA	July 16, 2020: **Advisory**[11]
Enterprise and Cloud Environments	No OPPA	No OPPA	No OPPA	July 1, 2021: **Advisory**[12]
Microsoft Exchange	July 19, 2021: **Statement**	July 19, 2021: **EU Declaration**	July 19, 2021: **Statement**	July 19, 2021: **WH Statement** & **Advisory** & **Indictment** & **State Statement**

7 In addition to the OPCW, Australia in this statement also attributed the targeting of "Malaysian locations participating in the Flight MH-17 investigation" (Minister for Foreign Affairs (2018): Australia condemns the cyber operations attributed to Russia against the Organisation for the Prohibition of Chemical Weapons (OPCW) and against Malaysian locations participating in the Flight MH-17 investigation as revealed by Dutch and UK authorities overnight).

8 Nevertheless, an EU Statement from October 4, 2018 referenced the UK attribution to the Russian GRU. A few days later, in the framework of the OPCW Executive Council, Germany took note of the incident and "call[ed] upon Russia to meet its international responsibilities and cease from such acts" (OPCW Executive Council (2018): Statement by H.E. Ambassador Christine Weil Permanent Representative of the Federal Republic of Germany to the OPCW at the Eighty-Ninth Session of the Executive Council). The Austrian intervention on behalf of the EU noted that "the offices of the OPCW were targeted by a hostile cyber operation carried out by the Russian military intelligence service" (OPCW Executive Council (2018): Statement on Behalf of the European Union Delivered by H.E. Ambassador Heidemaria Gürer Permanent Representative of Austria to the OPCW at the Eighty-Ninth Session of the Executive Council).

9 Germany did not use a communication channel to join this internationally coordinated OPPA. It has, however, previously issued an alert in May 2017, linking the CloudHopper operation to APT10 (Bundesamt für Verfassungsschutz (2017): BfV Cyber-Brief Nr. 02/2017). In a press conference on the day of the internationally coordinated OPPA, the deputy spokesperson of the Federal Government noted that Germany would have great confidence in the attribution of APT10 to Chinese government agencies made by various partner countries (own translation, Bundesregierung (2018): Regierungspressekonferenz vom 21. Dezember 2018).

10 A few days later, the U.S., the United Kingdom and Estonia reiterated the attribution to Russia's GRU following UN Security Council deliberations on the matter (United States Mission to the United Nations (2020): Joint Statement by Estonia, the United Kingdom, and the United States at a Press Availability on Russian Cyberattacks in Georgia). At the time, also Germany was a non-permanent member of the UN Security Council but did not join the authoring states. An EU Declaration from February 21, 2020 took note of the cyber operation against Georgian infrastructure, but did not include a political attribution.

11 Together with the United Kingdom and Canada.

12 Together with the United Kingdom.

Operation attributed	🇦🇺	🇩🇪	🇯🇵	🇺🇸
Ghostwriter	No OPPA	September 6, 2021: **National Statement** ↓ September 24, 2021: **EU Declaration**	No OPPA	No OPPA
Iranian APT I	November 17, 2021: **Advisory**	No OPPA	No OPPA	November 17, 2021: **Advisory**[13]
Ukraine I	February 20, 2022: **Statement**	No OPPA	No OPPA	February 18, 2022: **Press briefing**
Cyclops Blink	No OPPA	No OPPA	No OPPA	February 23, 2022: **Advisory**[14]
MuddyWater	No OPPA	No OPPA	No OPPA	February 24, 2022: **Advisory**[15]
Critical Infrastructure	April 20, 2022: **Advisory**	No OPPA	No OPPA	April 20, 2022: **Advisory**[16]
Ukraine II	May 10, 2022: **Statement**	May 10, 2022: **EU Declaration** ↓ **National Statement**	No OPPA	May 10, 2022: **Statement**
Iranian APT II	September 14, 2022: **Advisory**	No OPPA	No OPPA	September 14, 2022: **Advisory**[17]
DPRK Ransomware	No OPPA	No OPPA	No OPPA	February 9, 2023: **Advisory**[18]
KIMSUKY	No OPPA	March 20, 2022: **Advisory**[19]	No OPPA	No OPPA
CISCO Routers	No OPPA	No OPPA	No OPPA	April 18, 2023: **Advisory**[20]
Snake	May 9, 2023: **Advisory**	No OPPA	No OPPA	May 9, 2023: **Advisory**[21]

13 Joint advisory by Australia, the United Kingdom, and the U.S.
14 Together with the United Kingdom.
15 Together with the United Kingdom.
16 Joint advisory by Australia, Canada, New Zealand, the United Kingdom, and the U.S.
17 Joint advisory by Australia, Canada, the United Kingdom, and the U.S.
18 Together with South Korea.
19 Together with South Korea.
20 Together with the United Kingdom.
21 Joint advisory by Australia, Canada, New Zealand, the United Kingdom, and the U.S.

About Stiftung Neue Verantwortung

Stiftung Neue Verantwortung (SNV) is a non-profit think tank working at the intersection of technology and society. At SNV's core is a methodology of collaborative development of policy proposals and analyses. SNV experts do not work alone – they develop and test ideas together with representatives from politics and public administration, technology companies, civil society and academia. Our experts work independently of interest groups and political parties. We guarantee our independence through diversified financing, comprised of contributions from different foundations, state and corporate actors.

About the Authors

Christina Rupp is Project Manager for Cybersecurity Policy and Resilience at Stiftung Neue Verantwortung. Her work focuses on cyber diplomacy and cyber foreign policy, especially cyber norms, as well as Germany's cybersecurity architecture.

Dr. Alexandra Paulus is Project Director for Cybersecurity Policy and Resilience at Stiftung Neue Verantwortung. Her expertise covers cyber diplomacy, German and European cyber foreign policy, and cyber norms implementation. She leads SNV's cyber diplomacy projects.

Contact the Authors:

Christina Rupp
Project Manager Cybersecurity Policy and Resilience
crupp@stiftung-nv.de

Dr. Alexandra Paulus
Project Director Cybersecurity Policy and Resilience
apaulus@stiftung-nv.de

Imprint

Stiftung Neue Verantwortung e. V.
Beisheim Center
Berliner Freiheit 2
10785 Berlin

T: +49 (0) 30 81 45 03 78 80
F: +49 (0) 30 81 45 03 78 97

https://www.stiftung-nv.de/en
info@stiftung-nv.de

Design:
Make Studio
www.make-studio.net

Layout:
Alina Siebert