ANALYSIS

Germany’s Responses to Large Scale Malicious Cyber Incidents and Opportunities for AUS–GER future cooperation

Julia Schuetze, Project Manager Stiftung Neue Verantwortung, Berlin

November 2019

About the Author

Julia Schuetze is the Project Manager for International Cyber Security Policy at Stiftung Neue Verantwortung e.V. Her research focus is on joint responses to malicious cyber activities, specifically on cyber diplomacy of the European Union with the United States and Japan as part of the EU Cyber Direct project. She is a Cybersecurity Policy Fellow at New America Foundation. She has organized several workshops and events with cybersecurity experts from the U.S., EU, Japan and Germany in Washington D.C., Berlin and Tokyo to enhance international cooperation on cybersecurity. Prior to SNV, she worked at Wikimedia Deutschland e.V. and has researched at the Berkman Klein Center at Harvard University. She holds the Euromaster Transatlantic Track degree from University of Bath with stops at UW Seattle and HU Berlin. Her bachelor thesis at the University of Stirling, ‘Germany’s cyber security awareness programme: Lessons from the US’, was tutored by the German Federal Office for Information Security (BSI). She was also an intern at the Washington DC office of the Konrad-Adenauer-Foundation in 2014.

Large scale malicious cyber incidents have been on the rise. Classified as such are malicious activities with "significant impact[1]" that seek to undermine political integrity, national security and economic competitiveness, with the eventual risk of conflict.

Germany's Federal Office for Information Security (BSI) brings out a report about the state of IT-security every year. In 2019[2] it presented a threat situation affecting Germany, highlighting the increased risk of such large scale malicious activities that mirror two of the most consequential cyber incidents of 2017 WannaCry and NotPetya. Take NotPetya, a Ransomware attack[3] that exploited a widespread vulnerability in Microsoft affecting countries around the world and caused huge financial damage globally[4] and impacted Germany and Australia[5]. Since then, as BSI highlights in its 2019 report, more vulnerabilities were discovered, such as in a widely used chip hardware[6]. Ransomware attacks are still on the rise, a new form called Emotet has already affected German businesses and cities, halting services and production[7]. Moreover, digitalisation and digital dependability increase the effects of large scale attacks and widespread vulnerabilities. The effects are made worse due to the automation of attacks and therefore they could spread even more quickly globally and create massive economic damage; or in case of autonomous driving or attacks on medical devices, risk the health of people[8]. Moreover, the wider use of AI as a technology also bears new risks as AI can be hacked and has its own unique vulnerabilities[9].

Recognizing this threat landscape, governments have found different answers to respond to large scale malicious cyber activities, such as NotPetya. Most governments focus on the one hand on addressing the vulnerabilities and aim to increase resilience and cybersecurity, so those incidents cannot cause that much damage. On the other hand, governments are trying different strategies to influence the behavior of threat actors to punish them or prevent them from executing such incidents in the first place. The discussion on responses to malicious cyber activities spans the whole field of cybersecurity policy and becomes more and more part of the traditional security and foreign policy debates. This is because governments use a whole range of different policy instruments (military, regulatory, financial, technical, organizational and diplomatic) to respond to malicious cyber activities. Countries cannot do this in silos. Especially threats and vulnerabilities that cause large scale incidents, like NotPetya are global and therefore affect the cybersecurity of many countries. Accordingly, the global cybersecurity environment can be strengthened or weakened by actions taken by other governments. It can be weakened, for example if governments are using cyberspace as a means to achieve strategic geopolitical goals, such as damaging another country through a cyber attack as was found to be the case with NotPeyta[10]. This can weaken cybersecurity globally, since the vulnerabilities that are exploited for such an attack are in soft- and hardware that is used worldwide and thus makes other actors vulnerable. Moreover, if attacks are not targeted or executed as a targeted attack, the attack can spread quickly on its own, as was the case in NotPetya, soon affecting many businesses and public services in other countries. The global cybersecurity environment can however also be strengthened through international cooperation. For example, countries can assist each other in becoming resilient by sharing information about a threat quickly, working across borders with businesses on closing vulnerabilities that could be exploited for an attack. Those are just a few of the examples why it is important to think about the cybersecurity challenge with an international perspective.

Most countries therefore have by now set up a cybersecurity strategy that includes their international engagements and guides actions taken for cybersecurity or in cyberspace (see Australia, USA, Japan).

Understanding Germany's responses to large-scale malicious activities allows us to identify how Germany could work together with Australia as the strategic goals governments pursue as well as the policy instruments that they are using can offer opportunities and challenges for cooperation affecting bilateral and multilateral relations with other governments and international organisations.

The difference in the Australian and German government responses to malicious cyber activities can be best highlighted in the NotPetya incident that triggered many different political and especially foreign policy responses. Although both countries were affected, their foreign policy responses differed. This paper will examine Germany's responses (and how it does not respond) in comparison to other countries when it comes to large scale attacks like NotPetya. The focus of the analysis is Germany's domestic architecture[11] as well as the operational and foreign policy responses taken individually and jointly with other countries. Looking at this closer improves the understanding of what Germany's approach to cybersecurity is and its measures taken in case of a large scale cyber incident. It will moreover show some divergences to Australian responses but also opportunities for future cooperation with Australia.

Germany's responses to large scale malicious cyber activities

Germany takes a whole of government approach. This means that almost every federal governmental actor has some role in Germany's cybersecurity architecture[12]. The Federal Office for Information Security (BSI), responsible for Germany's IT-Security, specifically aims to complement this approach with a whole-of-society approach as a form of governance that engages the private sector, civil society, communities and individuals through different actions, such as information platforms or institutional dialogues. In the BSI's case, this approach was chosen to strengthen resilience and increase it-security for society and businesses more broadly.

When looking at the German government's responses to large scale malicious cyber activities, such as NotPetya in 2017, the main government agency at the centre of Germany's cybersecurity architecture, the **Federal Office for Information Security (BSI) is first and foremost responsible for the prevention and operational response of such large scale incidents**. To prevent large scale malicious cyber activities the German government focuses on the protection of critical infrastructure as well as government agencies' IT. This resulted in a regulatory response by implementing the IT Security Legislation[13] which demands a certain **set of standards and reporting mechanisms by critical infrastructure providers**. In order to facilitate a close and trustworthy relationship with its core stakeholder groups, such as businesses and governmental agencies, the BSI uses an **institutionalized dialogue** in the form of a public private partnership, the Alliance for Cybersecurity (AfCS/ACS). The AfCS is a network to share information on threats and protection mechanisms. In the case of NotPetya, BSI shared warnings and information on how to handle such an incident publicly as well as targeted by the AfCS[14]. It also does this preventatively as can be seen in a recent example when the BSI sent out a warning about the hardware chip vulnerability to all members of the Alliance for Cybersecurity and gave instructions for protection[15]. Ideally, this is to prevent the success of a large scale malicious activity that could use this vulnerability.

Another important element of Germany's response structure is the **National IT Situation Center (LZ) situated in BSI that is tasked to create an analysis of the threat environment for Germany and evaluate cyber incidents for state and private sector entities 24/7**. In a situation where an incident occurs experts at LZ react and distribute their analysis accordingly. In case of a large scale malicious activity, the LZ can become a crisis center. BSI may also gather and distribute information **via their Computer Emergency Response Teams or Mobile Incident Response Team that** in some very special cases may also provide technical assistance on the ground. For NotPetya and other larger incidents, another institution becomes very important for mitigating and reacting to the incident - the **Cyber Defense Center (NCAZ/ Cyber-AZ)**. It is housed by BSI but includes other government agencies, such as the federal police, the intelligence services, the armed forces -- mainly aiming to ensure a whole-of-government approach in operational response. Hence if a cyber threat occurs it is the place where the **operational response among different governmental bodies is coordinated**. Any information about the incident would be accumulated there and every government body represented would take appropriate steps, such as investigation, information gathering, technical assistance. This also occurred during the NotPetya incident[16].

Germany works with international partners on prevention of large scale incidents. For example since NotPetya the German BSI has published together with its counterpart in France, the National Cybersecurity Agency of France (ANSSI), a **common situational picture** that aims to inform the public but also helps the two countries be **better prepared and learn from each other**. It goes way beyond just information sharing. Such joint technical analysis can build a common understanding of threats and may be used by policymakers as a tool to inform their political analysis of the situation and ultimately the responses taken jointly. In their own words, the press statement reads as follows: "Both agencies agree that the threat situation concerning Ransomware is still alarming" and further it states "the impact, however is different in France and Germany, especially regarding global WannaCry and NotPetya ransomware campaigns in 2017. These different experiences regarding the consequences of the same attacks in the two countries emphasize the need to cooperate even closer, e.g. sharing information and jointly analysing cyber threats."[17] Hence joint technical analysis is used in response to large scale incidents with the aim to prevent and learn from other governments.

> **Due to the rise of cyber incidents despite the development of norms, the European Union has established a set of response mechanisms, including most prominently the so-called EU Cyber Diplomacy Toolbox which Germany supported through the Council decision adopted in June 2017.**

Looking specifically at Germany's foreign policy responses, its engagement and diplomatic efforts on cybersecurity, is centred traditionally around developing norms to increase the stability of cyberspace, freedom of expression and building capacity in other countries. For this, the German Federal Foreign Office (AA) created an International Cyber Policy Coordination Staff in 2011[18]. The AA is also involved in the German Cybersecurity Council that governs Germanys' strategy. Notably, the AA is not part of the Cyber Defense Center (Cyber-AZ) and thus has no part in the operational response in a large scale incident, like NotPetya. It rather aims to **prevent a large scale incident and increase the stability of cyberspace**, by engaging in **international fora for norm building, such as United National Group of Governmental Experts (UNGGE) and the Open Ended Working Group on Cyber Norms (OEWG)**. This foreign policy response is done jointly with other countries, for example since 2012 in strategic cooperation with Australia noted in the Berlin-Canberra Declaration of Intent on a Strategic Partnership where it states in Article 11: "Australia and Germany underline the importance of the Internet's security, its freedom and its potential for development, and share the view that there should be an appropriate balance between cyber security and access to information, freedom of expression and the protection of privacy. With a view to developing norms of state behaviour and confidence and security building measures for cyberspace, they will work closely together in international forums, particularly in the UN Group of Governmental Experts."[19] Hence, the foreign office's work has thus far mostly concentrated on prevention of large scale cyber incidents through norms in coordination with other countries.

Due to the rise of cyber incidents despite the development of norms, the European Union has established a set of response mechanisms, including most prominently the so-called EU Cyber Diplomacy Toolbox which Germany supported through the Council decision adopted in June 2017[20]. The EU Cyber Diplomacy Toolbox includes measures suitable for an immediate response to incidents as well as elements to encourage cooperation, facilitate the mitigation of immediate and long-term threats, and influence the behavior of potential aggressors in the long term. These measures range from diplomatic and political to economic actions to prevent, detect or react to malicious cyber activities, including those that do not rise to the level of internationally 'wrongful acts' but are considered as 'unfriendly acts'. This toolbox includes foreign policy tools including restrictive measures. Importantly, all those responses can only be implemented if all member states agree. With reference to

NotPetya, the Council passed the following conclusion[21] that Germany supported. The conclusion reads: “The EU firmly condemns the malicious use of information and communications technologies (ICTs), including in Wannacry and NotPetya, which have caused significant damage and economic loss in the EU and beyond. Such incidents are destabilizing cyberspace as well as the physical world since they can be easily misperceived and could trigger cascading events”.

Because getting all member states to agree is not the easiest task, countries have also chosen bilateral and multilateral coordinated or joint responses. Joint responses can be defined as an action that two or more countries take together in order to prevent, detect or react to malicious cyber activities including diplomatic instruments. A joint response to a specific threat or vulnerability or major incident includes the implementation of policy instruments. Here, beyond the European Union - level response to NotPetya, there are more and more responses by ‘coalitions of the willing and capable’ in reaction to major incidents where countries that agree to take further join together. Germany has so far not taken joint or coordinated bi- or multilateral responses in reaction to a major incident beyond supporting the EU Council’s decision. Examples of a coordinated response by a coalition of the willing and capable was seen, most prominently after NotPetya, where Australia led a coordinated attribution effort. In February 2018, within days of each other, seven nations including Australia attributed the NotPetya cyber attacks to Russia. It was no coincidence, according to Australia’s Ambassador for Cyber Affairs, Dr Tobias Feakin that ”[NotPetya] represented the largest coordinated attribution of its kind to date,” Feakin he said in April 2018 at the Australian Cyber Security Centre (ACSC) Conference in Canberra[22]. The governments of the US, the UK, Denmark, Lithuania, Estonia, Canada, and Australia called out Russia in official statements. Official statements of support came from New Zealand, Norway, Latvia, Sweden, and Finland. “That had followed also an additional coordinated calling-out of DPRK [North Korea] as responsible for the WanaCry incident,” Feakin said[23]. Germany did not join this coordinated attribution effort and there was also no official attribution by the German government individually done before or after the coordinated attribution. The German government was criticized in a news article for this as Handelsblatt had learned that the White House had shared confidential insights into the attack’s origins with German intelligence. A German government spokesman said the administration confined its statements on intelligence matters to the “responsible secret bodies of the German Bundestag”[24].

The German government has so far not been on the forefront of attribution. The only public attribution after a cyber incident was done by the Minister of Foreign Affairs in a press statement about the expulsion of Russian diplomats due to Scripal incident, an effort led by the United Kingdom. Here the Minister of Foreign Affairs added that the expulsion was also done due to the cyber incident that affected the foreign office in 2018, saying that it was most likely Russian actors that were responsible for the incident[25]. This was not a large scale cyber incident like NotPetya but a targeted attack infiltrating the foreign office. Public attribution to Russia had also been done frequently by the former Head of Germany’s Domestic Intelligence[26]. However, it can be disputed whether this is an actual public attribution by the German government as it was only communicated through media channels by himself and followed up by or embedded in embedded in other political actions or in a foreign policy approach towards Russia in an official German government statement.

Conclusion: Germany's responses to large scale malicious cyber incidents

Thus when it comes to foreign policy cooperation in reaction to a large scale incident, Germany is not cooperating openly or using the same response as Australia which has attributed frequently and is heading an international deterrence strategy right now. The German government, through its responses focuses mostly on prevention of large - scale cyber incidents and therefore its cooperation with other countries appears to be centred on that, too. Germany's foreign policy approach is still focusing on norms-building. Cyber incidents are not yet addressed as part of a broader foreign policy or security policy towards a country, for example with Russia. Germany has not yet published a cyber diplomacy strategy that would include or signal the use of diplomatic instruments as a response to cyber incidents. In case of non-existence of such a strategy, this may explain why Germany is not using diplomatic instruments, such as attribution, sanctions and more in response to a large scale incident. Therefore, Germany is not joining bilateral or multilateral cooperation to respond yet, like the coordinated attribution effort led by Australia. Strategically this could prove difficult in a world where cyber incidents are increasingly becoming part of broader geopolitical conflicts and are used as just another tool by some countries to undermine other countries' economies, national security and political integrity[27]. Unlike Germany's well-developed operational response which are also done together with other countries, like the join technical analysis that BSI and ANSSI put out, using other responses that are more political are underdeveloped. This is even more confusing in light of current debates on the use of offensive cyber means for defensive purposes, so-called active cyber defense, and attribution in Germany[28]. Without a clear international strategy that installs Germany's approach to cybersecurity and specific cybersecurity goals within its broader foreign and security policy goals, it would make the implementation and signalling of use of those instruments very unpredictable for like-minded governments and bad actors alike.

Opportunities for AUS-GER future cooperation

Taking into account the current state of Germany's responses to large scale incidents, there are three opportunities that emerge for further cooperation among Australia and Germany.

1. Firstly, Germany and Australia should **continue the dialogue on responses as it would help the understanding of options that are available to Germany and Australia** and will increase the awareness about under what conditions Germany may respond on EU level or on its own or potentially join a coalition of countries. This could help to coordinate responses in the future.
2. Secondly, Germany and Australia could **focus on threat analysis to prevent large scale cyber incidents.** Here both could learn from each other. starting with a common concern and common goal can assist in identifying options of closer cooperation. A specific common concern is for example threats to critical

infrastructure, and more specifically threats from cyberspace that could halt the successful implementation of energy transition that both countries have in common. In Australia, renewable energy is growing at a per capita rate ten times faster than the world average. The next fastest country is Germany[29]. The assumption made by the German government that energy transition "means that access to them is less likely to lead to conflicts[30]" and further that "it will also be more difficult for states to use energy sources to exert pressure" should be discussed again taking into account the unique vulnerabilities that renewable energy systems have[31] and that in general energy infrastructures are becoming increasingly the target of cyber attacks[32]. Since Germany and Australia have an interest in a successful energy transition, a common goal could be to address the cybersecurity implications in this context and analyse specifically threats to energy transition and evaluate what responses may be useful to mitigate them.

3. Thirdly, Germany and Australia should start **working together not just on norm development but on norm implementation and aim to support global governance cooperation platforms to achieve the implementation of norms**. Many norms have been/are being developed in different fora. For example the UN established two intergovernmental processes on cybersecurity – the Open Ended Working Group (OEWG) on developments in the field of information and telecommunications in the context of international security, and the sixth Group of Governmental Experts (GGE) on developments in the field of information and telecommunications in the context of international security. Germany and Australia are members of both groups. Then multi-stakeholder initiatives, such as the Global Commission on the Stability of Cyberspace (GCSC) recently launched its final report, which offers a cyber stability framework, principles, norms of behaviour, and recommendations for the international community and wider ecosystem. Further there is the Paris Call for trust and security in cyberspace that was signed by Germany and Australia. What is necessary now, is an initiative that oversees the implementation of norms worldwide and identifies actions to ensure norm implementation. As both countries support the multistakeholder approach to internet governance, a pledge to support a global digital cooperation architecture as a way to support norm implementation could aid bringing stakeholders together. The High-level Panel on Digital Cooperation was convened by the UN Secretary-General to advance proposals to strengthen cooperation in the digital space. Three ways of achieving this goal were proposed in the report and are now being further developed and discussed worldwide. All have strengths and weaknesses as a German multi-stakeholder group has identified in a workshop in October 2019[33]. The Australian government put out a public statement commenting on the recommendations[34]. A beneficial next step for norm implementation could be to use those two discussions, one on digital cooperation architecture and one on norms for cyberspace and identify what sort of architecture Australia and Germany would pledge to support to implement norms or develop norms further.

Endnotes

[1] EU definition that governs the implementation of EU Cyber Diplomacy toolbox that Germany passed in Council with all other member states. Council of the European Union (2019) Cyber-attacks: Council is now able to impose sanctions

[2] BSI (2019) Die Lage der IT-Sicherheit in Deutschland 2019

[3] Greenberg (2018) The Untold Story of NotPetya, the Most Devastating Cyberattack in History

[4] Greenberg (2018) The Untold Story of NotPetya, the Most Devastating Cyberattack in History

[5] BSI (2017) Update: Cyber-Angriffswelle Petya – Bedrohung größer als bekannt or Scherchel (2017) BSI-Warnung: Nach wie vor hohe Gefahr durch NotPetya-Backdoor in MeDoc or Minister for Law Enforcement and Cyber Security (2018) Australian Government attribution of the 'NotPetya' cyber incident to Russia

[6] Reichert (2019) Hardware vulnerability bypasses Spectre and Meltdown patches

[7] Westernhagen (2019) Trojaner-Befall: Neue Emotet-Welle legt Neustädter Stadtverwaltung lahm

[8] BSI (2019) Die Lage der IT-Sicherheit in Deutschland 2019

[9] Herpig (2019) Attack surface of machine learning

[10] Russia used NotPetya incident to and then it spread

[11] Herpig and Bredenbock (2019) Cybersicherheitspolitik in Deutschland. Akteure, Aufgaben und Zuständigkeiten. Im Fokus: Das Cyber-Abwehrzentrum

[12] See Germany's cybersecurity architecture here: https://www.stiftung-nv.de/sites/default/files/cybersicherheitspolitik_in_deutschland.pdf

[13] Bundesanzeiger (2015) IT-Sicherheitsgesetz

[14] BSI (2018) Die Lage der IT-Sicherheit in Deutschland 2018

[15] BSI (2019) Windows-Schwachstelle: BSI warnt vor möglichen wurmartigen Angriffen

[16] BSI (2018) Die Lage der IT-Sicherheit in Deutschland 2018

[17] BSI (2018) ANSSI and BSI present their first "Common situational picture"

[18] Federal Foreign Office (2019) International cyber policy

[19] Australian Government Department of Foreign Affairs and Trade (2012) Berlin-Canberra Declaration of Intent on a Strategic Partnership

[20] European Council (2017) Cyber attacks: EU ready to respond with a range of measures, including sanctions

[21] Council of the European Union (2018) Council conclusions on malicious cyber activities

[22] Stilgherrian (2018) Blaming Russia for NotPetya was coordinated diplomatic action

[23] Stilgherrian (2018) Blaming Russia for NotPetya was coordinated diplomatic action

[24] Koch (2018) Germany is just fine with the NotPetya cyberattack but its allies aren't

[25] Auswärtiges Amt (2018) Bundesregierung zum Fall Skripal

[26] Reuters (2018) German intelligence sees Russia behind hack of energy firms: media report or Russia 'was behind German parliament hack' or Reuters (2017) Germany challenges Russia over alleged cyberattacks

[27] See for example: Center For Strategic International Studies (2019) Significant Cyber Incidents and Tallait (2019) Disrupt and restraint: The evolution of cyber conflict and the implications for collective security

[28] Herpig (2019) Aktive Cyber-Abwehr: Innenminister schaltet bei IT-Sicherheit schrittweise von Verteidigung auf Angriff

[29] https://theconversation.com/australia-is-the-runaway-global-leader-in-building-new-renewable-energy-123694

[30] Maas (2019) Speech by Foreign Minister Heiko Maas at the opening of the Berlin Energy Transition Dialogue

[31] Stamper et al (2017) Distributed Energy Systems: Security Implications of the Grid of the Future und Idaho National Laboratory (2016) Cyber Threat and Vulnerability Analysis of the U.S. Electric Sector

[32] See: Sanger und Perlroth (2019) U.S. Escalates Online Attacks on Russia's Power Grid, E-ISAC (2016) Analysis of the Cyber Attack on the Ukrainian Power Grid and Cimpanu (2019) Ransomware incident leaves some Johannesburg residents without electricity

[33] Heumann, Göhlich, Schuetze (2019) Workshop Documentation UN High-Level Report – discussing Architectures for global digital Cooperation

[34] Australian Government Department of Foreign Affairs and Trade (2019) IGF Consultation: Report of the UN Secretary-General's High-level Panel on Digital Cooperation

Editor

Katja Theodorakis

Publisher

Konrad Adenauer Stiftung (Australia) Limited
Regional Programme Australia and the Pacific

11/3 Sydney Avenue
Barton, ACT 2600
Australia

Tel: +61 2 6154 9322

www.kas.de/australia

Disclaimer

All rights reserved. No part of this publication may be reprinted or reproduced or utilised in any form or by any electronic, mechanical or other means, now known or hereafter invented, including photocopying or recording, or in any information storage or retrieval system, without permission from the publisher.

The opinions expressed in this publication rests exclusively with the authors and their interpretations do not necessarily reflect the views or the policy of the Konrad Adenauer Stiftung.

Design, Layout and Typeset

Swell Design Group

Paper

FSC
www.fsc.org
RECYCLED
Paper made from
recycled material
FSC® C102086

ecoStar+ is an environmentally responsible paper. The fibre source is FSC Recycled certified. ecoStar+ is manufactured from 100% post consumer recycled paper in a process chlorine free environment under the ISO 14001 environmental management system.