10 Cyber securities and cyber security politics

Understanding different logics of German cyber security policies

Stefan Steiger

The internet has rapidly become an integral part of everyday life in modern societies. While it has helped to facilitate economic growth and cultural exchange, it has also become a new domain for conflict. The increasing sophistication of cyberattacks is politically challenging, as the internet has become the meta-infrastructure of modern societies – a “backbone of backbones” (Choucri and Clark 2012: 151). Today, information technology (IT) influences almost every aspect of social life. Though many states have established cyber security¹ policies, emphasizing their claim to protect the nation and the citizens not only offline but also in cyberspace, the regulation of cyber security is especially complex because of the different actors involved (including both state and non-state) and the international reach of the internet that makes unilateral regulation difficult. Moreover, national decisions regarding cyber security (e.g. the stockpiling of vulnerabilities) can affect actors around the world.

States have dealt differently with these new opportunities and challenges. While some have actively employed offensive cyber capabilities as a substitute for conventional intervention, others have used cyber capacities in complement with more traditional responses to threats. Yet, cyber security policy is not just a military issue that relates to interstate conflict dynamics; it also has the potential to have a lasting impact on the relationship between state authorities and citizens, as well as between states and companies. Therefore, the expansion of state competences in cyberspace has not remained unchallenged. Interventions into the private lives of citizens or entrepreneurial freedom have sparked substantial domestic opposition. Internationally, practices of mass surveillance conducted by intelligence agencies have received considerable criticism. However, it has remained largely unclear which factors, both domestic and foreign, influence different cyber security policies. Since most IR theories tend to focus on either international (i.e. realism) or domestic (i.e. liberalism) dynamics, significant aspects of policies that hinge on the interplay of those two spheres are not accounted for. Thus, scholars have called for approaches that consider both domestic and international influences on cyber security policy, as well as how they interact (Whyte 2018: 12). This chapter employs a role theoretical, two-level game to analyze the

development of German cyber security policy. This approach facilitates a more nuanced view on cyber security policies and considers both the domestic and international dynamics that shape cyber security policies.

This chapter therefore addresses the following question: How did German cyber security policy evolve and what domestic and external factors facilitated its development? The policies under examination will be taken from four areas central to cyber security: Critical infrastructure protection, law enforcement, intelligence services, and the military. Each of these subject areas are significantly shaped by different kinds of uncertainty (for example, evaluating the potential risk of attacks and the benefits of undermining IT security). In addition, responsibility for these domains is often split between state agencies and – especially in the case of critical infrastructure protection – non-state actors. This results in varying policy responses and dynamics between different actors in each field. Furthermore, an examination of German cyber security policies is especially interesting, as a gap exists within the literature concerning the cyber security strategies of states with a cautious foreign policy approach. Most theory-driven studies have focused on developments in the United States and sometimes China or Russia (Dunn Cavelti 2008; Fritz 2017; Maréchal 2017; McCarthy 2018).

To answer the research question, this chapter draws on the symbolic interactionist role of theory in foreign policy analysis (FPA) and traces policy developments relying on a corpus of policy documents from the executive as well as other state agencies and from non-state actors. The chapter proceeds as follows: First, the theoretical premises of role theory are presented, and the concept of a two-level role play is outlined. Following this, essential interactions in the four fields of activity are analyzed. Finally, a short conclusion summarizes the findings.

Role theory

Roles have been increasingly used as analytical concepts for studying foreign policies.² Following the symbolic interactionist strain in role theory, roles are understood as social positions that are shaped by ego and alter expectations, and that are associated with a function for a social group (Harnisch 2012: 8). Roles are defined relationally; stable social relationships depend on a role and a complementary counter-role. For example, if an actor claims the role of protector (as the government does in cyber security policy), another actor must fill the role of the one needing protection. However, this relationship does not require any rational complementarity of interests. The motives for assuming role and counter-role may be different and are not immediately relevant for the resulting social structure, as social reality emerges from role interaction (Harnisch 2014: 14).

Though traditional role theory assumes homogeneous and nationally accepted role conceptions, this has changed in recent years. The insight that roles can be disputed domestically between different actors, for example between governments and citizens, has led role theoreticians to develop the concept of role contestation

(Cantir and Kaarbo 2012). Various empirical studies have since traced the influence of domestic role contestation on a nation's foreign policy behavior (Cantir and Kaarbo 2016). However, some analytical blind spots remained. For example, the repercussions of international interactions on the domestic social structure still required more investigation. Therefore, a holistic role theory approach was developed that connects the international process of role and counter-role taking with a domestic role play ("Full-spectrum role-taking"; Harnisch 2014). Examining both levels of role creation is inspired by the two-level game of Robert Putnam (1988), but offers two main advantages: First, it is not limited by a formalistic reference to treaty ratification, but can portray different forms of interaction. Second, the focus is not on balancing two rationalist win-sets, but on the interconnectivity of roles in the different spheres:

The model suggests that the two role-taking processes are interactive: international role taking and making feeds back into domestic role taking (second image reversed) and domestic role taking enables and/or restrains external role taking.

(Harnisch 2014: 2)

Building on this foundation, this chapter argues that there is a domestic role play between government, legislature, judiciary, the private sector, and other non-state actors, and an international role play concerning other states, institutions, and NGOs. Furthermore, the German government has domestically claimed the role of protector in cyberspace, but still requires a complementary counter-role to facilitate a stable cyber security policy. Although the role of protector is not the only role the German Executive plays domestically (another example might include welfare maximizer), it is the most relevant for cyber security and therefore deserves dedicated analysis. Since there are different significant others involved and the role of protector can apply to different actors in different situations, it should be noted that role interaction patterns vary across the different areas of investigation.

Figure 10.1 Two-level role play.

The development of cyber security policies

The following sections illustrate that the development of cyber security policies differ considerably between the four areas analyzed. This is due to the international and domestic interactions between the government and different significant others. The first section shows that, with regard to critical infrastructure, the role of protector was first delegated to the private sector but has since been reclaimed by the government. The second section illustrates that the government is still struggling to establish a stable protector role regarding cybercrime and is actively embroiled in domestic contestation processes with law enforcement agencies. The third section reveals that, while the conduct of the German intelligence service BND has been criticized following the Snowden revelations, many practices have since been deemed legal due to the value of this information internationally. The final section explores the evolution of the government's role as protector of the military, eventually adopting a more offensive stance toward combating cyber security threats in line with the needs of NATO allies.

From delegation to control: The protection of critical infrastructures

In 1997, the German Federal Government began work on the protection of critical infrastructures. Initially, the government founded a Critical Infrastructures Working Group (Schulze 2006: 155–156), which recommended close cooperation between “business, science and politics” (Ressortarbeitsgruppe KRITIS 1999). Parliamentarians also assessed that this task should be jointly managed by both the state and industry. The operators of critical infrastructures should also be encouraged to establish appropriate security management of the assets (Deutscher Bundestag 1998: 17). However, these findings remained largely inconsequential at first. The policy for the protection of critical infrastructures gained real traction only after the 9/11 terror attacks. Subsequent anti-terrorism legislation passed by the government highlighted the vulnerability of critical infrastructures to cyberattacks and strengthened the Federal Office for Information Security (BSI). In addition, the cooperation KRITIS, which was intended to enable the state and economy to exchange information effectively, was founded in 2002. However, experts found the network proved largely deficient (Schulze 2006: 185, 247).

In 2005, the government presented the “National Information Infrastructure Protection Plan”, the first strategic document for the protection of critical (information) infrastructures in Germany (Bundesministerium des Innern 2005: 3). Though the plan assigned responsibility for the protection of infrastructures primarily to private sector operators, the German government (in close consultation with industry) would define minimum standards that would guarantee an adequate level of protection against cyberattacks (Bundesministerium des Innern 2005: 13). The KRITIS implementation plan, published in 2007, continued this approach of voluntary cooperation and recommended various measures to be taken by companies. However, the central tenet of the infrastructure protection strategy remained

that “the goal should be reached in consensus between the private sector objectives of the operators and the overriding (welfare) interest of the community” (Bundesministerium des Innern 2007: 5). As such, in this first phase of German infrastructure protection, the protector role was delegated to operators of critical infrastructures.

However, cooperation between the state and the private sector fell short of the government’s expectations. From the administration’s point of view, companies did not comply with their obligation to provide information and neglected their duties to establish suitable standards. In addition, Stuxnet made clear that attacks on industrial targets were no longer just hypothetical scenarios (Bundesministerium des Innern 2011: 3). As a result, the government debated introducing binding regulations that would provide better protection of critical infrastructures. Federal Interior Minister Friedrich said:

I know that there are voices in the economy that would prefer to cooperate on a voluntary basis. However, experience shows that in the past we have been behind our goals with voluntary measures alone. We need a legal framework for more cooperation and compliance with IT security standards.

(Bundesministerium des Innern 2013)

This marked the departure from the government’s reliance on voluntary cooperation and more strongly bound the protector role to state authorities. With the IT Security Act passed in 2015, the government obliged companies to comply with minimum standards and to report substantial cyberattacks. The new law thus significantly strengthened the supervisory competence of the BSI (Bundesamt für Sicherheit in der Informationstechnik 2016: 5). Although the industry associations eco and Bitkom supported the ultimate goals of the law, there was substantial criticism of the government’s decision to abandon the previous regulatory arrangement. Companies initially objected to the interference in entrepreneurial freedom and potential overregulation (heise.de 2013; eco 2015: 3). Efforts to stop the IT security law, however, were unsuccessful.

From about 2012, the government increasingly prioritized securing critical infrastructures internationally as well. Following the establishment of the first voluntary principles for the protection of critical infrastructures by the G8 in 2003 (G8 2003), there was increased interest across the EU in regulating the protection of critical infrastructures (European Commission 2009). Yet, discussions on the introduction of EU rules protecting critical infrastructures only started to take shape in 2013. Together with other states also pursuing standards for the handling of critical infrastructures, Germany worked toward the adoption of the Directive on security of network and information systems (NIS Directive). Like the German IT Security Act, the NIS Directive provides for state supervision of critical infrastructures and establishes reporting obligations (European Union 2016). In parallel with developments in the EU, Germany also promoted the protection of critical infrastructures within the OSCE. As early as 2011, the government supported “the obligation to protect critical infrastructures” in a proposed code of conduct, which

was also introduced in the UN (United Nations 2011: 9). In 2016, a second round of confidence-building measures related to critical infrastructure protection were adopted within the OSCE under German chairmanship. These additional measures addressed the possibilities for more voluntary cooperation in the protection of cross-border infrastructure (OSCE 2016a).

In Germany's case, international cooperation on the protection of critical infrastructures was only possible after the domestic role of protector was firmly established and clear among all actors. Furthermore, it is no coincidence that this cooperation emerged in regional organizations because of the physical interconnectedness of critical infrastructures. Knowing the minimum standards of other nations and understanding how other actors engaging in the protector role view their position, reduces the uncertainty with regard to cascading effects across borders.

New methods of investigation and domestic contestations: Law enforcement

Germany established the first legal basis to make computer fraud and interference with data integrity criminal offenses in 1986. These changes, supported by the administration's claim that these laws will protect economic well-being, were hardly contested domestically. Yet, as the internet grew into a global phenomenon, it became increasingly clear that a nationally bound protector would be insufficient against the wide scope of threats the internet may introduce. To guarantee effective law enforcement against a transnational force, transnational solutions must be sought (Bundesregierung 1999). Consequently, the government began to engage with like-minded states on the international level. One of the main goals was to avoid conflicts as a result of diverging criminal laws (Brodowski 2015).

As cybercrime represented a significant problem for many states by the late 1990s, legal frameworks for law enforcement agencies were put in place in countries around the world. Much of this legislation shared significant similarities and attempted to address similar problems. Across legislative regimes, both the threat (cyberattacks) and the threatening actor (non-state criminal actors) were typically defined and labeled in similar ways. Early international coordination efforts included the establishment of a committee of experts within the Council of Europe in 1997. The committee was tasked with drafting the first international convention to counter cybercrime. The resulting Budapest Convention was opened for signature in 2001 and outlines a series of criminal offenses that signatories are required to transpose into national law. The compatibility of the national protective roles also enabled the harmonization of criminal law within the European Union. Particular mention should be made of framework decision 2005/222/JHA, and its eventual replacement, directive 2013/40/EU. Despite increasing coordination between states, including the establishment of transnational investigative powers for combating cybercrime, central authority in law enforcement (as well as the responsibility for specific regulations) still rests with individual EU member

states (Brodowski 2015: 268; Hilgendorf and Valerius 2012: 36–37; Council of Europe 2001).

The complexities of navigating two levels of cybercrime response, conforming to both international and domestic expectations, is well-illustrated when examining the German case more closely. Two factors have been influential: first, the ongoing domestic debate about which actor is ultimately responsible for ensuring sufficient protections against cybercrime, about who should take on the protector role, makes it difficult to negotiate further international cooperation. Second, a resolution to these debates has been hindered by the reluctance of the government to delegate or share parts of the protector role.

The struggle to establish clear limits, and a clear understanding, of what the protector role of the German government should be intensified after terror attacks in Madrid (2004) and London (2005). To keep pace with technological development, the government provided law enforcement agencies with two tools to enable lawful interception: source telecommunications monitoring (Quellen-TKÜ) and online search (Online-Durchsuchung) (Deutscher Bundestag 2006). The use of these measures created substantial resistance within German society, as many critics considered IT devices to be at the core of private life and thus covert investigations represented a disproportionate invasion of privacy. In July 2007, representatives of civil society and the Left Party filed a constitutional complaint against online search. In February 2008, the Federal Constitutional Court ruled that this measure was admissible only “if there were actual indications of a specific danger to a legally protected interest of paramount importance”. The court further defined “the fundamental right to ensure the confidentiality and integrity of information technology systems”. In addition, the court requested that an online search could only be conducted with a judicial warrant, restricting its use as a cybercrime prevention tool (Bundesverfassungsgericht 2008). The domestic debate further intensified when, in 2008, the Chaos Computer Club revealed that the software used to conduct lawful interception was much more powerful than it was supposed to be. The software was not limited to intercepting communications prior to encryption as intended, but in fact enabled the complete monitoring of infected devices (CCC 2011). Even though domestic disputes about the appropriate powers of state institutions have been fierce, the German government has repeatedly stressed the importance of the new investigative tools to deal with serious crime and terrorism (Deutscher Bundestag 2017: 24586).

With reference to these challenges, the government reduced the thresholds for using Quellen-TKÜ and online searches in 2017. This step has led to substantial and ongoing criticism (heise.de 2017). Clearly, the scope and powers of the government, the self-appointed protector, in German society is still hotly debated. As long as there is no stable role relationship domestically, it is very difficult to negotiate international rules regarding the same issues. Additionally, the protector role is considered to be at the core of state functionality and therefore has clear limits on how much can be delegated to other actors. Therefore, unlike the protection of critical infrastructure, the establishment of a stable domestic role relationship may not result in substantial international cooperation.

Between criticism and dependency: The German intelligence service

When Edward Snowden revealed the extensive surveillance measures of the NSA and GCHQ in June 2013, Germany found itself in the position of being spied on by some of its closest allies. Chancellor Merkel's initial remarks reflected much of German society's reaction to this reveal: "spying among friends is not at all acceptable" (Spillius 2013). Following the revelations, the government attempted to convince the United States to renounce espionage activities against Germany and proposed a bilateral agreement to this end. However, these efforts were largely ignored by the United States. This alienated Germany and prompted Berlin to initiate increased activities in the field of counterintelligence (Bundesregierung 2015). This introduced a new, and critical, element to the government's protector role; never before did Germany require protection from the actions of its allies.

Since the United States did not respond to bilateral solutions, the German administration resorted to other means to ease domestic outrage. In order to counter the United States' privileged physical access to internet traffic, thereby making espionage more difficult, the construction of a new transatlantic undersea cable was launched in cooperation with Brazil. As a result, less internet traffic would be routed through the United States (Reuters 2014). Germany and Brazil were also responsible for co-sponsoring a UN resolution against excessive surveillance activities in the digital age (United Nations 2013). But even in this context direct confrontation with the United States was avoided. Thus, the text of the resolution was substantially watered down in consultations (Reuters 2013).

As the scope of the allegations became clearer, there was mounting domestic pressure for a thorough investigation of the events. For this reason, the German Bundestag set up a Committee of Inquiry in March 2014. In parliamentary debates and on the part of the government, however, it was repeatedly pointed out that Germany relied on security cooperation with the United States and that this relationship could not be jeopardized by harsh criticism (Bundesministerium des Innern 2014). In particular, Germany could not conduct the intelligence-gathering it required for its security without using data gathered by the United States and other allies (Deutscher Bundestag 2013a, 2013b). For all intents and purposes, Germany had at least partly outsourced its protector role to the United States.

The work of the Committee of Inquiry soon revealed that the practices of the NSA were not the only problem. It became increasingly obvious that the German federal intelligence service (BND) were employing similarly questionable practices in the name of security. The Committee's investigation and the documents disclosed by Edward Snowden revealed, for example, that the BND cooperated with the NSA regularly and substantially, and that data of German citizens were exchanged (Mascolo 2014). As the extent of the government's activities became more widely understood by the public, attention shifted toward the domestic sphere. Members of the political opposition and representatives of civil society accused the government of disproportionate surveillance activities. From a role theoretical perspective, the allegation was that the administration had expanded its role without significant others even knowing.

Domestic criticism in Germany was so intense that the government had to reorganize the legal framework governing foreign intelligence. In 2016, the administration submitted a new law that was meant to bolster the legal justification for the BND. To achieve complementary counter-role taking by parliament and to appease the public, this included new control mechanisms as well as special protections not only for Germans but also for citizens of the European Union. This demonstrates that Merkel's statement about spying among friends may have held weight, and that the protector is only under limited circumstances allowed to act against certain allies. However, the new law also legalized many of the questionable practices uncovered during investigations. Consequently, the law has been subject to considerable criticism from lawyers, the parliamentary opposition, civil society, and even international organizations like the OSCE (OSCE 2016b). Nevertheless, the BND Act was passed by the Bundestag in October 2016. The government had successfully negotiated the expansion of its protector role within an increasingly hostile environment. Furthermore, the experiences of sobering interactions with international partners resonated in the debates (Deutscher Bundestag 2016b: 19625).

Government officials emphasized that for this very reason the legislation was designed not to limit the BND in its operations, but instead to create transparent regulations (Deutscher Bundestag 2016a: 18274). However, the BND and the government's support of the agency continues to attract criticism. In January 2018, an alliance of civil society actors filed a constitutional complaint against the BND Act that has yet to be resolved; it is possible that a ruling by the Federal Constitutional Court might force the government to act again (Reporter ohne Grenzen 2018). At least in part because of ongoing criticism, the government has increasingly outsourced elements of its protector role to its allies, to both capitalize on the efficacy of existing intelligence sources as well as respond to the limits put on its domestic capabilities. This expansion remains contested domestically.

From defense to offense: Military cyber security

In 2007, the German armed forces established a unit assigned to computer network operations (CNO). This marks the first military effort to protect the Federal Republic in cyberspace, and was the first move toward the development of offensive capabilities. The task of this new unit was to operate in computer networks of enemies and, if necessary, complement or replace conventional military operations (Deutscher Bundestag 2014: 1165). The risks of military hostility in cyberspace nonetheless kept the government critical of a militarized cyberspace. Thus, the administration argued for promoting a "culture of restraint" ("Kultur der Zurückhaltung"). This included a prohibition on the development of malware by the German *Bundeswehr* (Deutscher Bundestag 2010: 5). The role of protector thereby remained inconsistent; on the one hand the *Bundeswehr* should be able to conduct CNOs, but on the other, it should not engage in the practice of developing related tools.

Following this path of self-restraint, the Bundeswehr's responsibilities (largely limited to defense) were described in Germany's first cyber security strategy (Bundesministerium des Innern 2011: 5). While this new role for the protector was not contested, parliamentarians claimed that offensive cyber measures would require a constitutive mandate of the Bundestag – just like conventional deployments. The government subsequently reassured that CNOs were governed by the same rules as more traditional warfare (Deutscher Bundestag 2015b: 4). In addition, the government confirmed that Article 26 of the Basic Law also prohibits a war of aggression in cyberspace (Deutscher Bundestag 2015b: 7).

On the international level, however, efforts to encourage states to exercise self-restraint have found little resonance. Although Germany was substantially involved in UN discussions regarding IT and international security (UN GGE), the government was not able to successfully lobby for a culture of restraint. In fact, despite its posturing for restraint on the international stage, capacities of the German Armed Forces significantly expanded after 2010. Furthermore, early positions regarding the development of offensive technologies were apparently abandoned. Even though the government initially stated that the *Bundeswehr* would not develop malicious software, in 2015 the administration confirmed that the CNO forces had to resort to the exploitation of vulnerabilities to operate in enemy networks (Deutscher Bundestag 2015a: 11–12). While the government argued that vulnerabilities that could have “far-reaching implications for the security of the population or the state” should be disclosed, it nevertheless made clear that such disclosure may not interfere with the government's capability to enact its role as a protector (Deutscher Bundestag 2018: 10). The development of offensive capabilities nevertheless signifies a substantial change in policy and armed the protector with the capabilities necessary to (offensively) act in cyberspace. The growth of capacities was mirrored by expanding claims for protection. While the tasks of the *Bundeswehr* were initially focused on the protection of military infrastructure, cyberspace became an increasingly acceptable domain for military action in the years that followed. The buildup of cyber capacities culminated in 2017 when the German Armed Forces established a new cyber command (Bundesministerium der Verteidigung 2016).

Two processes facilitated the expansion of the military's protector role: first, the German government followed in the footsteps of its international “significant others”. In particular, demands and developments in NATO were particularly influential. NATO recognized cyberspace as “a domain of operations in which NATO must defend itself as effectively as it does in the air, on land, and at sea” at the Warsaw Summit in 2016 (NATO 2016). The establishment of a cyber command in 2017 was considered necessary to ensure effective cooperation with allies. Second, the new tools and capabilities were continually justified by the growing number and sophistication of cyberattacks (Bundesministerium der Verteidigung 2016). The Minister of Defense specifically pointed out that cyberattacks were used in complement with conventional forces in Georgia in 2008 and supported hybrid warfare in Ukraine (Bundesministerium der Verteidigung 2015).

The offensive use of cyberspace remains a contentious issue. Critics argue that the peaceful use of the internet is threatened, and that stockpiling vulnerabilities undermined the security of the global system (FIFF 2015; Gesellschaft für Informatik 2015). Against the international pressures, however, the challenges from civil society remain inconsequential.

The ambiguity of the military's protector role is emphasized when the goal of restraint is contrasted with the subsequent buildup of offensive capabilities. It is evident that the process of establishing a more capable protector undermines lofty ideals about restraint in the international system. The actions taken by the German Armed Forces directly contradicted its purported goal, and if other states took similar actions, an international culture of restraint would be made far more difficult to achieve. For example, while international law regulates a visible distinction between combatants and non-combatants for armed forces, the government emphasizes that cyber warfare does not require such a distinction. Although the use of false identities is prohibited (e.g. to direct suspicion onto other actors), the wide acceptance of the use of concealment tactics nevertheless makes it difficult to build a verifiable culture of restraint in cyberspace (Deutscher Bundestag 2015b: 11). Driven by the demands of international significant others and an increasingly dangerous cyberspace, the government's protector role started to undermine the initial goal of restraint.

Conclusion: The different logics of German cyber security policy

This chapter has argued that German cyber security policy is a multifaceted phenomenon characterized by different patterns of interaction in the four areas studied. The analysis has illustrated that the areas of investigation are characterized by different constellations of actors (significant others) that are affected by both domestic and external influences. The approach of a two-level role play takes this into account. The different patterns of international and domestic interactions were found to constitute a variety of "protector roles" the government may attempt to fulfill, though the different spheres were influential to varying degrees. Considering German cyber security policies in total, it is evident that the Government of Germany has successfully and significantly extended the scope of its protective role. It has done so by expanding the competences of different security institutions and by centralizing control of assets like critical infrastructures. But a closer look reveals a more fragmented and nuanced picture.

The most significant source of international cooperation has been related to the protection of critical infrastructures. After unsatisfactory domestic cooperation with companies led to the creation of binding regulations, similar arrangements were pushed for and implemented at the EU level. Reducing the protector's domestic commitments by delegating to the private sector enabled more substantial international cooperation. International coordination also proved useful in relation to law enforcement; the harmonization of criminal law between states is

facilitated by the similarities between protector roles in different states. In cases where domestic role contestation is ongoing, for example regarding criminal procedural law, the potential benefits of international cooperation are less clear. In fact, it is this unstable domestic role relationship that impedes useful international cooperation.

Nevertheless, in both areas the protector attempted to regulate the behavior of non-state actors (including companies and criminals). When it comes to self-binding regulations, a different picture emerges. The Snowden revelations illustrate the changing dynamics between domestic and international spheres of role playing. Germany's protector role was simultaneously threatened by the United States' activities, which could not be successfully curtailed, but also bolstered by continued access to the information those questionable practices uncovered.

It was the reluctance of international partners, together with an increasingly dangerous cyber environment and a growing demand for more autonomy domestically, that led the German government to establish a more far-reaching legal basis for foreign surveillance and thereby expand its protector role. The government's success in this matter is even more notable since the Snowden revelations also exposed the BND to substantial criticism, resulting in ongoing role contestation within Germany. With regard to the Armed Forces, the Federal Republic started to work toward an international culture of restraint toward military activities in cyberspace, but here, too, the actions of international partners forced Berlin's hand. In order to fulfill its protector role and meet requirements of NATO, the Federal Republic has set up its own military cyber command and initiated a buildup of capacities after 2010, thereby at least partially undermining the ultimate goal of restraint. Domestic contestations in this area remained largely inconsequential.

Within the larger context of international cyber security, it is clear that even states considered cautious in their foreign policy pursuits can aggravate the challenges of transnational cyber security. Germany's foreign intelligence service is highly capable and is known to analyze internet traffic as it passes German internet exchange points. The government also resorts to stockpiling vulnerabilities and, if necessary, operating covertly in cyberspace. Even though a decision has not yet been made regarding the responsible disclosure of vulnerabilities, it is clear that from a governmental point of view, some vulnerabilities are essential in order to effectively perform the protector role. Resorting to covert action, including purposefully complicating attribution efforts, directly undermines the explicitly stated goal of a verifiable culture of restraint, since even attacks from more cautious states will occur hidden.

Notes

- 1 The term "cybersecurity policy" refers to political practices aimed at ensuring the confidentiality, integrity, and availability (CIA-triad) of data and data processing systems and to those policies undermining these goals of IT security.
- 2 For an overview of foreign policy role theory, see Harnisch (2018); Breuning (2017).

References

All links checked on August 23, 2021.

- Breuning, M. (2017). Role Theory in Foreign Policy. In *Oxford Research Encyclopedia of Politics*. <https://doi.org/10.1093/acrefore/9780190228637.013.334>.
- Brodowski, D. (2015). Cybersicherheit durch Cyber-Strafrecht? Über die strafrechtliche Regulierung des Internets. In H.-J. Lange and A. Böttcher (eds), *Studien zur Inneren Sicherheit: Band 18. Cyber-Sicherheit*. Wiesbaden [Germany]: Springer VS, pp. 249–276.
- Bundesamt für Sicherheit in der Informationstechnik. (2016). Das IT-Sicherheitsgesetz: Kritische Infrastrukturen schützen. Retrieved from: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/IT-Sicherheitsgesetz.pdf?__blob=publicationFile&v=7.
- Bundesministerium der Verteidigung. (2015). Keynote der Verteidigungsministerin auf dem Kolloquium des Cyber-Workshop. Retrieved from: <https://www.bmvg.de/de/themen/dossiers/weissbuch/perspektiven/keynote-von-ministerin-von-der-leyen-beim-cyber-workshop-11028>.
- Bundesministerium der Verteidigung. (2016). Abschlussbericht Aufbaustab Cyber- und Informationsraum. Retrieved from: http://docs.dpaq.de/11361-abschlussbericht_aufbaustab_cir.pdf.
- Bundesministerium des Innern. (2005). Nationaler Plan zum Schutz der Informationsinfrastrukturen. Retrieved from: https://www.innenministerkonferenz.de/IMK/DE/termine/to-beschluesse/05-12-09/05-12-09-anlage-nr-16.pdf?__blob=publicationFile&v=2.
- Bundesministerium des Innern. (2007). Umsetzungsplan KRITIS: des nationalen Plans zum Schutz kritischer Infrastrukturen. Retrieved from: https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/it-digitalpolitik/umsetzungsplan-kritis.pdf?__blob=publicationFile&v=4.
- Bundesministerium des Innern. (2011). Cyber-Sicherheitsstrategie für Deutschland. Retrieved from: https://www.cio.bund.de/SharedDocs/Publikationen/DE/Strategische-Themen/css_download.pdf?__blob=publicationFile.
- Bundesministerium des Innern. (2013). Friedrich stellt Wirtschaft IT-Sicherheitsgesetz vor. Retrieved from: https://www.bmi.bund.de/SharedDocs/kurzmeldungen/DE/2013/03/eco_mmr_itsicherheitsgesetz.html.
- Bundesministerium des Innern. (2014). Rede von Bundesinnenminister de Maizièrè anlässlich des 11. Symposiums des Bundesamtes für Verfassungsschutz am 8. Mai 2014 in Berlin. Retrieved from: <https://www.bmi.bund.de/SharedDocs/reden/DE/2014/05/bfv-symposium.html>.
- Bundesregierung. (1999). Rede des Bundesministers des Innern, Otto Schily, bei der Konferenz der Bertelsmann-Stiftung “International Internet Content Summit 1999”: Weltweite Kommunikation - eine neue Kultur gemeinsamer Verantwortung. Retrieved from: https://www.bundesregierung.de/Content/DE/Bulletin/1990-1999/1999/58-99_Schily.html.
- Bundesregierung. (2015). Sommerpressekonferenz von Bundeskanzlerin Merkel. Retrieved from: <https://www.bundesregierung.de/Content/DE/Mitschrift/Pressekonferenzen/2015/08/2015-08-31-pk-merkel.html>.
- Bundesverfassungsgericht. (2008). Urteil vom 27. Februar 2008 –1 BvR 370/07. Retrieved from: https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2008/02/rs20080227_1bvr037007.html.