Germany’s Perspective on Cyber Security Policy Making
Some Thoughts

Stefan Heumann, Stiftung Neue Verantwortung

Germany’s growing footprint in International Affairs

Much ink has been recently spilled on Germany’s growing international footprint. Analysts have been impressed with the strength and resilience of the Germany economy during and in the aftermath of the financial crisis of 2008. During the Euro-Crisis German power and leadership within the EU was both berated and praised. Her visibility and her calm but firm management of the Euro crisis pushed chancellor Angela Merkel into the international spotlight. And her bold decision to keep German borders open during the height of the refugee crisis in Europe cemented her status and the role of Germany as the key player within the EU. While during the past decades Brussels had emerged at the place where the most important decisions in Europe are taken, everyone was reminded that the road to a decision in Brussels leads through Berlin. Thus when the election of Donald Trump as President of the United States surprised (and shocked) many around the world, those worried about the future of the liberal order quickly turned their head towards Angela Merkel and expressed hopes that she would somehow fill the void. Many of these analyses greatly overestimate the ability and the power of Angela Merkel and Germany to step into international leadership roles that a Trump presidency is leaving unfilled. But there is no doubt. During the past decade Germany’s influence – both within the EU and on the global stage – has become more visible. This has not only triggered debate about Germany’s role in international affairs. It has also lead to controversy within Germany on how the country’s interests and values should shape its foreign policy.

The Tension between Civil Liberties and Security

The perception of growing German influence in foreign affairs forms the broader context for my thoughts on how the German government is grappling with some fundamental tensions and challenges in cyber security. The core of the tension lies in Germany’s constitutional and legal historical traditions which have emphasized the protection of civil liberties and fundamental rights – including the right to privacy – and the growing awareness of policy makers that Germany needs to take more responsibility for its security in an increasingly volatile international environment. The discussions in Berlin about the fallout of the Snowden revelations put this tension on full display. On the one hand government officials and the broader public expressed outrage and concern about the violation of civil liberties and privacy by large-scale surveillance programs. On the other hand the Snowden revelations exposed Germany’s dependence on the US for intelligence and security. Two decades after the end of the Cold War and political disagreements over the war in Iraq or the conduct of the “War on Terror” this dependence has increasingly become a sore spot among the wider public and even among committed trans-Atlanticists. Thus the Snowden revelations also served as a “wake-up call” for many government officials worried about Germany’s ability to provide for its own security. But if Germany wants to reduce its reliance on the publicly maligned NSA, it has to expand its own surveillance capacities. This tension between Germany’s legal institutions, which for important historical reasons put a premium on the protection of privacy as a fundamental right and its growing international responsibilities, which – in the eyes of many – require stronger defense and intelligence capabilities shapes German debates over cyber security.
Cyber Security Policy in Germany

Cyber security is not a new area for policy making in Germany. The Federal Office for Information Security (BSI) was already established in 1991, turning the former cryptographic unit of Germany’s foreign intelligence agency (BND) into an entirely separate agency under the auspices of the Ministry of Interior. The establishment of this new agency with the sole mission to help protect German information networks and systems signaled that the German government recognized the new challenges of the coming information age. And the creation of this new civilian agency entirely separate from the foreign intelligence agency also underscored the government’s commitment to strong encryption as a foundation for trust and cooperation between the BSI and German (IT) industry.¹ But until a few years ago only experts knew about the work of the BSI. The field of information or cyber security was seen as highly technical, an area for computer and IT experts but not a field of strategic importance for high-level government officials and policy makers. As a consequence of the cyber attacks on Estonia in 2007 Germany published its first national cyber security strategy in 2010, resulting in the creation of the Cyber Defense Center and the National Cyber Security Council in the following years. And the discovery of the Stuxnet malware in 2010 also received broad media coverage and attention in Germany. But those events did not really change the predominant thinking that cyber security was a highly technical field that should be left to IT experts.

This did not really change until the Snowden revelations hit Germany. Information security suddenly made national headlines. The reports about NSA surveillance programs and their implications for Germany culminated in the story about the tapping of Chancellor Merkel’s cell phone. The German government had to respond. Cyber security became elevated from a technical issue of a highly specialized largely unknown government agency to a top priority on the agenda at the German Chancellery and at Cabinet meetings. The scale and reach of the NSA programs changed the debate about the Internet and digital technologies in Germany. Even those still skeptical of the importance of the digital revolution now began to realize its geostrategic importance. International coverage of the debate in Germany largely focused on the concerns over privacy. But the Snowden revelations had a much deeper impact on Germany. They also changed the government’s perspective on security and industrial policy. The security debate focused on two big areas. On the one hand there was the concern about information security both in and outside of government. On the other hand there was also the question of how German security agencies should use the Internet to gather intelligence and improve national security. The Snowden revelations also highlighted the dominance of US technology companies. Thus the debate on industrial policy was driven by concerns of Germany’s dependence on foreign technology and IT companies – a debate often lead under the buzzword “technological sovereignty.” And this debate is closely related to a larger debate on how digital and connected technologies are transforming German industry, economy and society. In 2014 the German government adopted the so-called “Digital Agenda” – a high-level policy document on how the government seeks to promote the development and adoption of digital technologies in government, the economy and society.

During the past four years government officials have realized that cyber-security is central to Germany’s economic and security interests. I do not seek to give a comprehensive overview here. I just would like to sketch especially those initiatives that help understand how Germany

¹ https://lawfareblog.com/germanys-crypto-past-and-hacking-future
is approaching cyber security policy making and that are also interesting from a perspective of international engagement and discussion.

**New German Foreign Intelligence Law**
The German parliament started its own inquiry into NSA surveillance in 2014. In the end, much of the work of the committee focused on the German foreign intelligence agency BND. Major problems were identified in the course of the committee’s work, most notably the lack of effective oversight and legal mandates for its work. The debate resulted in the adoption of a new intelligence law. The new law seeks to address some of the main shortcomings in oversight. But it also codifies into law a broad mandate for foreign intelligence collection by the BND. My colleague Thorsten Wetzling analyzed some of the most important elements of the intelligence reform in a paper summed up in this lawfare article.2

**New IT Security Law adopted in 2015**
The new IT Security Law is focused on the protection of critical infrastructures in Germany against cyber threats. Companies providing critical infrastructure in seven sectors (IT and Telecommunications, Energy, Health, Transport, Food, Water, Finance and Insurance) are supposed to develop and implement IT security standards in cooperation with the BSI. Any company that is classified under the new law as critical infrastructure also needs to meet new obligations to report significant cyber attacks or IT incidents on their systems.

**Government Hacking**
The Snowden revelations also lead to a broad debate in Germany about the importance of encryption to protect information. At the same time the threat of terrorist attacks has also alerted the government to the need of security agencies to monitor and access digital communications of suspects. Contrary to some reports in the media, German government officials have so far not backed away from any commitment to strong encryption. But the German government is doubling down on hacking as an alternative to get access to information. This year it passed a highly controversial amendment to the government hacking law. It has also created a new technical agency that is supposed to provide law enforcement and domestic security agencies with technical tools to gain access to targets’ communications (through the exploitation of security flaws in the implementation of encryption or exploitation of other soft- and hardware vulnerabilities. This approach requires policies for the management of vulnerabilities (guidelines and risk assessments to make decisions regarding acquisition, retention and disclosure of vulnerabilities) – a policy that is currently still lacking in Germany.

**German Military’s New Cyber Command and the “Hack-Back” Debate**
This year the German military created a new cyber command, highlighting the importance of the cyber domain in military conflict. The new cyber command is an important step in consolidating German military cyber capabilities. At the same time, many international and domestic observers perceive this step as a step towards a more offensive-oriented rationale. But this perceptions stands in sharp contrast to the low numbers of actual personnel dedicated to offensive capabilities. The “hack back” debate is not confined to the military. It is part of a larger debate in Germany about active cyber defense measures and their implications for national and international law as well as the question which agency or office should be responsible for under what kind of guidelines and oversight.

---

Protection of Political IT Infrastructures, especially in the Context of Elections

This is a fairly new issue on the agenda but one that has received high-level attention from government officials and is frequently discussed in the media. Ever since the DNC hacks and the subsequent leaks of the sensitive emails, government officials have been concerned that hacks and leaks and disinformation campaigns more broadly could have an impact on the German election. While the widely anticipated hacks and leaks have not materialized and while there is no evidence of a large scale disinformation campaign that goes beyond the fake news that is mostly shared among rightwing social media outlets, cyber security in the context of political campaigns and elections has emerged as new central issue in German cyber security policy.

Conclusion

It is not until quite recently that Germany has begun to turn cyber security policy into an important political priority. But once it realized its strategic importance to its economic and national security interests, the German government has really shifted gears and is seeking to catch up with other countries whose cyber security policies are more advanced. German officials are especially interested in the rich cyber security eco systems in Israel and the United States and the interplay between public and private sector within them. As cyber security has become the new game in town, there are also growing turf battles within the German bureaucracy. Civilian, law enforcement and military departments, agencies and offices are competing for resources and responsibilities in a policy area that they all perceive as one of growing importance and prestige. And cyber security expertise is currently in dire demand across the entire government. But there is also a unique opportunity here. Moving later offers the opportunity to learn from the countries that moved first. And rather than activism across and competition between numerous government agencies Germany needs a debate about its cyber security architecture as a whole. How do you divide role and responsibilities across government agencies and encourage coordination in cyber security policy making? And how do you draw the line and find the right balance between defensive and offensive cyber capabilities? Whoever sits in the next German government will grapple with these larger questions. And there is great interest in Germany to learn from the lessons of other countries. What is out of the question is that cyber security policy making will only continue to grow in importance.