Germany Develops Offensive Cyber Capabilities Without A Coherent Strategy of What to Do With Them

AP Photo – Michael Probst

Germany has traditionally prioritized defense over offense in cyberspace. That's now beginning to change.

There is a reoccurring debate in German national security and foreign policy whether Germany suffers from "Strategieunfähigkeit"—an inability to develop and implement strategy. The historic trauma of two lost World Wars created a pacifist culture that always struggled with formulating national security interests and defining strategy. The so-called "culture of reluctance" regarding the use of hard power has bled into Berlin's thinking about cyber issues, especially as it rushes to develop capabilities without an overarching strategy on how to use them.

Until recently, Germany has prioritized defense over offense in cyberspace. The Federal Office for Information Security (BSI), Germany's cybersecurity agency, has a strictly non-military defensive mandate and is a vigilant advocate of strong encryption and full disclosure of zero-day vulnerabilities to vendors. Germany's foreign intelligence agency (BND) has historically had a relatively small cyber

espionage budget.

Germany's defensive posture began to shift in 2015, after the internal network of the German Bundestag was successfully compromised by Russian state-backed operators. That led the country to revise its cybersecurity strategy, issuing a more offensive-minded document in 2016. It called for the development of cyber teams in the intelligence agencies. It also might have been a contributing factor to the creation of a specialized agency, called the Central Office for Information Technology in the Security Sphere (ZITiS), to develop innovative techniques to break into encrypted devices, develop exploits and malware for real time interception and accessing data at rest, as well as identify or purchase zero-days to support offensive capabilities.

As Germany rolled out its 2016 strategy, the German military (Bundeswehr) centralized its cyber capacity by consolidating around 14,000 soldiers and IT personnel into a unified cyber command (CIR), loosely modelled on U.S. Cyber Command. CIRwants to achieve full operational capacity by the early 2020s and plans to perform strategic and tactical cyber operations against enemy assets. Usage scenarios include disrupting enemy military assets, battlefield support and reconnaissance on adversary IT assets.

Through the new strategy, the meaning of cybersecurity in Germany shifted from strengthening IT-security to improving public safety through the use of offensive cyber operations.

Berlin's latest move favoring offensive cyber activity is the creation of a cyber innovation agency, akin to the United States' DARPA, announced in August 2018. Its mandate is to conduct market research and sponsor promising projects with potential value for cyber offense and cybersecurity. Over the next five years, the agency is supposed to be equipped with a budget of €200 million (roughly $227 million), 80 percent of which will fund research projects—a substantial sum considering that the entire budget of the BSI is only €120 million per year.

These developments over the last three years point to a build-up of Germany's offensive cyber capability. Interestingly, these new capabilities have been created without having a clearly defined strategic purpose—a problem that has plagued German national security policy in the past. For example, during the 2001 NATOmission in Afghanistan, Bundeswehr capabilities—designed for

territorial defense from invasion—were not well adapted or flexible enough for an expeditionary mission.

This mismatch between strategy and capabilities plagues Berlin's approach to cyberspace. There is currently no strategic debate about what German policymakers want to achieve with its new offensive capabilities. Questions about attribution and appropriate responses have apparently not yet been discussed. It is further unclear whether the political will exists to use these offensive capabilities in a time of crisis. For example, if deterring cyberattacks by punishment is a goal, strategy should make clear what means, including non-cyber options, would be most suitable. Is offensive cyber activity more useful in deterring adversarial cyber operations as say indictments or economic sanctions? Currently government officials seem to simply assume that cyber capabilities alone have a deterrent effect without taking into consideration the strategic requirements that come with deterrence by punishment, namely credibly holding assets at risk and signaling desired behavior while being willing to face consequences in case of an escalation. Will Germany indeed launch a retaliatory cyberattack against adversaries that provoke it and in turn face the potential consequences of entering an escalation cycle with, say, Russia or China?

As Germany tries to flex its muscles in cyberspace, allies and adversaries alike will be left to wonder what to expect absent an overall strategy. German policymakers should start a strategic discussion about the country's role in a contested cyberspace. It needs to explain to its allies how its new offensive tools will work to support multilateral frameworks like NATO, the EU and the UN. Germany also needs to signal to hostile cyber actors what behavior it deems inappropriate, and how it will likely respond if certain red-lines are crossed.

- Matthias Schulze is an associate at the German Institute for International and Security Affairs (SWP). FULL BIO
- Sven Herpig is the project director for the Transatlantic Cyber Forum at Stiftung Neue Verantwortung (SNV). FULL BIO

Source:
https://www.defenseone.com/ideas/2018/12/germany-develops-offensive-cyber-capabilities-without-coherent-strategy-what-do-

them/153227/?oref=d-nextpost?oref=d1-related-article

[Disclaimer]