No. 30
October 2022

DGAP POLICY BRIEF

A Reliable Global Cyber Power

Cyberspace and Germany's National Security Strategy

Dr. Valentin Weber
Research Fellow,
Technology and Global
Affairs Program

Germany's major allies have declared their roles in shaping cyberspace. The United States sees itself as a *democratic*, values-driven cyber power ready to impose substantial costs on adversaries engaged in nefarious conduct. The United Kingdom strives to be a *responsible* cyber power that eschews reckless behavior. France aims to operate as a *stabilizing* power that counters a destructive Russia and other malicious actors. But what kind of cyber power is Germany to be? As it draws up its first national security strategy, the country can rectify its lack of vision and narrative for its domestic and international cyberspace efforts. This policy brief proposes that Germany espouse a sober focus on reliability that links its cyberspace strategy to those of its allies, thereby providing a vital anchor for Western cybersecurity. To do this, Germany should:

– **Defend countries that look to it for support and build capacities to provide that assistance.**

– **Consistently promote strong and transparent cybersecurity to encourage partners abroad to adopt policies that do the same.**

– **More prominently declare that it has offensive cyber capabilities and that it would deploy them for defensive purposes in accordance with international law.**

– **Share offensive cyber capabilities with trusted partners, if requested, in crisis situations.**

INTRODUCTION

Russia's invasion of Ukraine gives Germany a unique opportunity to position itself on the global cyberspace stage. It must go beyond its simple declarations of conducting cyber operations in accordance with international law and its commitment to pursue capacity building. Such anodyne statements are incomprehensible to Germany's allies, especially in times of crisis. Berlin instead needs to take action that fits a strategic narrative. In short, it is time for the country to take a stance as a (cyber) power and shed a reputation for unreliability.

Germany has always pictured itself as a good partner, part of a *Bündnis* (alliance) with Western powers. But German politicians now increasingly believe that their country needs to stand out from the pack, assume leadership, and wield military and security capabilities that match its economic power. Attaining these goals requires an ability to transform into a *reliable* cyber power, one that protects vulnerable European neighbors, showcases effective domestic policies that can be emulated internationally, and offers offensive cyber capabilities that complement those of other major cyber powers. These capabilities include tools of war that, also in peacetime, can stop malicious cyber operations.[1] Pursuing such policies is less about deterrence (Iran repeatedly launches cyberattacks on the United States despite its declared and demonstrated offensive capabilities) than about the proper conduct of a transparent democracy that is accountable to its citizens. Russia has never publicly acknowledged its offensive cyber capabilities or explained the circumstances under which it uses them.

Germany, above all, cannot afford more navel-gazing about the meaning of the *Zeitenwende* and its implications for a post-Cold War identity. The country needs to move on to a national security strategy (NSS) with all the attributes of a "grand strategy," including a clear narrative that informs and motivates German society. The NSS must incorporate the cyber efforts of its allies and address their deficiencies, and the first step in accomplishing this is understanding their positions in the cyber domain.

THE UNITED KINGDOM: THE RESPONSIBLE CYBER POWER

The United Kingdom notes in its 2021 Integrated Review of Security, Defence, Development and Foreign Policy that it is not only a leading cyber power but also a responsible one.[2] It consequently conducts cyber operations that conform with international and domestic law. This includes the Intelligence Services Act of 1994, which instituted parliamentary oversight of the country's intelligence services. British cyber capabilities, the Review states, are also proportionate and targeted, limitations that are part of the United Kingdom's effort to diametrically oppose "irresponsible" cyber behavior. The Review singles out Russia as a country that acts this way in cyberspace since it does not assess the legality of its cyber operations that have caused widespread, if not global, collateral damage.[3] The United Kingdom, as a responsible cyber power, openly declares its offensive capabilities. "We will continue … to declare our nuclear and offensive cyber capabilities to Allies' defense under our [NATO] Article 5 commitment."[4]

FRANCE: THE STABILIZING CYBER POWER

France, in its 2021 strategic update, positions itself "[a]s a stabilising power dedicated to peace and security." The document also states that "[France] promotes effective multilateralism that respects human rights, fundamental freedoms and democratic principles."[5] The country has adopted a stance to counter destabilizing forces, including Russia, which is developing "exotic" weaponry. This includes nuclear-powered cruise missiles and intercontinental nu-

1 Valentin Weber, "Rethinking European Cyber Defense Policy," German Council on Foreign Relations, (April 2022): <https://dgap.org/sites/default/files/article_pdfs/dgap-policy%20brief-2022-08-en.pdf> (accessed September 30, 2022.

2 The Cabinet Office, *Global Britain in a Competitive Age: The Integrated Review of Security, Defence, Development and Foreign Policy*, (March 16, 2021): <https://www.gov.uk/government/publications/global-britain-in-a-competitive-age-the-integrated-review-of-security-defence-development-and-foreign-policy> (accessed September 30, 2022).

3 Monica Kaminska, James Shires, and Max Smeets, "Cyber Operations during the 2022 Russian invasion of Ukraine: Lessons Learned (so far)," European Cyber Conflict Research Initiative (July 2022): <https://eccri.eu/wp-content/uploads/2022/07/ECCRI_WorkshopReport_Version-Online.pdf> (accessed September 30, 2022.

4 *The Cabinet Office, Global Britain in a Competitive Age*, p. 20.

5 Ministry of the Armed Forces, *Strategic Update*, (2021), p. 45: <https://www.stjornarradid.is/library/03-Verkefni/Almannaoryggi/Thjodaroryggismal/France%20-%20Strategic%20Review%202021.pdf> (accessed September 30, 2022.

clear torpedoes.[6] France also seeks to spearhead international stabilization efforts, even in regions in desperate need of political reform. France includes in its definition of stability the right to respond to cyberattacks.[7] Its posture in this regard is akin to the United Kingdom's as both defend norms of responsible state behavior. France also strives to safeguard stability by using confidence-building measures to staunch potentially escalatory effects of cyberattacks.

THE UNITED STATES: THE DEMOCRATIC CYBER POWER

The United States positions itself as a values-driven defender of democratic norms. As such, it may sometimes blur the stipulations of international law to pursue its own geopolitical aims. Regarding the principle of sovereignty,[8] the United States has noted that "a State's remote cyber operations involving computers or other networked devices located on another State's territory do not constitute a *per se* violation" of sovereignty.[9] Such a perspective is broader than France's, for example, which considers "any unauthorized penetration by a State of a French system or *any* production of effects on French territory via a digital vector" as a violation of sovereignty (emphasis added).[10]

The United States' self-image as a cyber power is also characterized by a willingness to impose serious costs on adversaries, an approach that is part of the persistent engagement theory that has driven recent US efforts in cyberspace:

"*Defending forward as close as possible to the origin of adversary activity extends our reach to expose adversaries' weaknesses, learn their intentions and capabilities, and counter attacks close to their origins. Continuous engagement imposes tactical friction and strategic costs on our adversaries, compelling them to shift resources to defense and reduce attacks.*"[11]

US President Joe Biden's 2021 National Security Strategic Guidance is also unique in its heavy emphasis on values. It states that cyber threats, like other threats, are ultimately targeted against a community of democracies.[12]

A TRIO OF ISSUES

There are three problems with the positioning of the three powers. First, they are not as coordinated as they may initially appear. Although their strategy documents often use the same language, the countries interpret wording differently. All three, for instance, share a general *applicability* of international law to cyber operations, but considerable differences about *how* the law applies exist. The aforementioned example about the definition of sovereignty highlights this.

Second, the three powers routinely overestimate the factors behind their unity, whether on international norms or as a community of values. They could consequently find themselves bound together even if the behavior of one is seen by the others as "irresponsible" or "destabilizing." In one scenario, the United States, having placed malware into an adversary's critical national infrastructure and missile systems, compromises that state's offensive and defensive capabilities, thereby triggering preemptive action by

6 Ibid.

7 Secrétariat Général de la Défense et de la Sécurité Nationale (SGDSN), *Revue stratégique de cyberdéfense* [Strategic Cyberdefense Review], (February 12, 2018), pp. 86-87: <http://www.sgdsn.gouv.fr/uploads/2018/02/20180206-np-revue-cyber-public-v3.3-publication.pdf> (accessed September 30, 2022).

8 For context on international law and the principle of sovereignty in cyberspace, see Isabella Brunner, Erich Schweighofer, and Jakob Zanol, "Malicious Cyber Operations, 'Hackbacks' and International Law: An Austrian Example as a Basis For Discussion on Permissible Responses," *Masaryk University Journal of Law and Technology* 14, no. 2, (September 23, 2020): <https://journals.muni.cz/mujlt/article/download/13187/11652> (accessed September 30, 2022).

9 United Nations General Assembly, *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* (July 13, 2021), p. 140: <https://front.un-arm.org/wp-content/uploads/2021/08/A-76-136-EN.pdf> (accessed September 30, 2022).

10 Ministry of the Armed Forces, *Droit International Appliqué Aux Opérations Dans Le Cyberespace* [International Law Applied to Cyberspace Operations], (2019): <https://www.justsecurity.org/wp-content/uploads/2019/09/droit-internat-appliqu%C3%A9-aux-op%C3%A9rations-cyberespace-france.pdf> (accessed September 30, 2022).

11 U.S. Cyber Command, "Achieve and Maintain Cyberspace Superiority: Command Vision for US Cyber Command," (2018), p.6: <https://assets.documentcloud.org/documents/4419681/Command-Vision-for-USCYBERCOM-23-Mar-18.pdf> (accessed September 30, 2022.

12 "We will stand with our allies and partners to combat new threats aimed at our democracies, ranging from cross-border aggression, cyberattacks, disinformation, and digital authoritarianism to infrastructure and energy coercion." The White House, "Interim National Security Strategic Guidance," (March 2021), p. 19: <https://www.whitehouse.gov/wp-content/uploads/2021/03/NSC-1v2.pdf> (accessed September 30, 2022).

that adversary.[13] Conducting disruptive operations on allied territory could also be perceived as illegitimate action.[14]

Third, each of the powers often frames its own role primarily in the negative, in terms of what they are not. France does not operate like a terrorist group because terrorist groups are spoilers and destabilizers. The United States is not like China because the two countries' values are diametrically opposed to one another. The United Kingdom is not like irresponsible Russia. Even when positive doctrines are elaborated, they are muddled. The United Kingdom speaks of "responsible offensive cyber operations" in its aims to hold malicious cyber actors accountable for their activities.[15] But the author of this DGAP Policy Brief has previously noted that conducting "responsible" cyber offensive operations is illusive due to definitional and operational challenges.[16]

GERMANY: THE RELIABLE CYBER POWER

The conclusion from this analysis is that the cyberspace strategies of Germany's allies significantly overlap in their overarching goals. Differences, however, emerge over the applicability of international law and the conduct of cyber operations. The United States is the boldest by far concerning disruptive operations – Stuxnet and interference with North Korean missile capabilities come to mind – while France and the United Kingdom have adopted a more restrained or, at least, secretive approach.[17] This perceived discrepancy in boldness needs to be reflected in national strategies. Germany's NSS should lay out the many commonalities it holds with allies, but Berlin should also highlight its distinction as a reliable cyber power. Here is how Germany should do this.

At Home …

Germany's NSS and domestic policies must be reliably and consistently geared toward transparency and strong cybersecurity to encourage policies abroad that emphasize the same. Its current policies regarding vulnerability disclosure and encryption do not do this. The interior ministry's recent cybersecurity agenda emphasizes the role of the Central Office for Information Technology in the Security Sector (ZITiS) in the domestic development of offensive cyber tools to reduce reliance on similar foreign instruments.[18] However, unlike the United States and the United Kingdom, Germany lacks a transparent policy on publicly disclosing the use of such tools.[19] Without such a framework, known commonly as a "vulnerabilities equities process," in place, Germany fails to protect itself and others since it sets an example for opacity.

Germany's domestic policy on encryption is similarly unworthy of a reliable cyber power that boasts strong security. The country's current approach can be summed up as "security through encryption and security despite encryption."[20] This reflects contradictory German objectives of upholding end-to-end encryption while undermining it by allowing authorities to have backdoor access. Such a policy exposes Germany to cyber threats and further legitimizes the actions of authoritarian states that have systematically weakened encryption to allow domestic surveillance.

13 Daniel Moore, *Offensive Cyber Operations: Understanding Intangible Warfare* (London, 2022).

14 Chris Bing, "Command and Control: A Fight for the Future of Government Hacking," *Cyberscoop*, April 11, 2018: <https://www.cyberscoop.com/us-cyber-command-nsa-government-hacking-operations-fight> (accessed October 3, 2022).

15 The Cabinet Office, *Global Britain in a Competitive Age*, p. 42. Another problem is that the United Kingdom's Integrated Review cites several examples of responsible cyber offensive behavior, but they entail only actions against non-state actors, which is not a distinguishing factor of a democratic cyber power. This is because Russia and China may undertake similar action against terrorists or sexual abuse of children just as democracies do. The only example in the United Kingdom's document that seems to concern nation-state actions relates more to defensive capabilities to keep "UK military aircraft safe from targeting by weapons systems." (p. 42) Examples of the United Kingdom as a responsible power in the conduct of offensive cyber operations against other *state actors* are otherwise missing from the Review.

16 Valentin Weber, "The Illusion of 'Responsible' Cyber Offense," German Council on Foreign Relations (October 27, 2021): <https://dgap.org/en/research/publications/illusion-responsible-cyber-offense> (accessed September 30, 2002).

17 Jon R. Lindsay, "Stuxnet and the Limits of Cyber Warfare," *Security Studies* 22, no. 3 (2013), pp. 365–404: <https://doi.org/10.1080/09636412.2013.816122> (accessed September 30, 2022); David E. Sanger and William J. Broad, "Trump Inherits a Secret Cyberwar Against North Korean Missiles," *The New York Times*, March 4, 2017: <https://www.nytimes.com/2017/03/04/world/asia/north-korea-missile-program-sabotage.html> (accessed September 30, 2022).

18 Bundesministerium des Innern und für Heimat, "Cybersicherheitsagenda des Bundesministeriums des Innern und für Heimat" [The Cybersecurity Agenda of the Federal Ministry of the Interior and Community], (June 2022): <https://www.bmi.bund.de/SharedDocs/downloads/DE/veroeffentlichungen/themen/sicherheit/cybersicherheitsagenda-20-legislatur.pdf?__blob=publicationFile&v=4> (accessed September 30, 2022).

19 Deutscher Bundestag, "IT-Schwachstellenmanagement der Bundesregierung" [Federal Government IT Vulnerabilities], January 25, 2022: <https://www.bundestag.de/presse/hib/kurzmeldungen-879150> (accessed September 30, 2022); Government Communications Headquarters, "The Equities Process," November 29, 2018: <https://www.gchq.gov.uk/information/equities-process> (accessed September 30, 2022).

20 Bundesministerium des Innern, für Bau und Heimat, "Cybersicherheitsstrategie für Deutschland 2021" [Cybersecurity Strategy for Germany 2021], (August 2021): <https://www.bmi.bund.de/SharedDocs/downloads/DE/veroeffentlichungen/2021/09/cybersicherheitsstrategie-2021.pdf;jsessionid=C6B367B55F7F2C0AD403FB31F2C5A9CA.2_cid322?__blob=publicationFile&v=2> (accessed September 30, 2022).

... and Abroad

Germany's cyber vision needs to align with its overall vision of itself as a power or, in other words, with its grand strategic goals.[21] Current strategic priorities lie in playing a greater role in European defense and, in this area, being a reliable partner for its weaker neighbors. Indeed, Germany has recently taken a more active role in patrolling Eastern and Southeastern European airspace, specifically that of Poland and Romania, areas directly threatened by Russia.[22]

Germany should assume a similarly active role in defending the Eastern and Southeastern European flanks in cyberspace and coordinate this effort with other EU member states. To do this, the country will need to increase international capacities and exchange best practices with partners. Recent cyberattacks on Albania (which it has attributed to Iran) reveal the need for regional cyber defense support,[23] which has, in the aftermath of the cyberattacks, come primarily from the United States.[24] In Montenegro, also a target of malicious cyber activities, the US Cyber Command has assisted in making networks more resilient.[25] Demand for German expertise, however, also exists. Staff from Germany's Federal Office for Information Security, in fact, were scheduled just before Russia's invasion to travel to Ukraine to deliver cybersecurity support. While security considerations made the trip too risky, such assistance is to be encouraged under safer circumstances.

Germany's statement on offensive capabilities is hidden on page 133 in the definitions section of its 2021 cybersecurity strategy. Berlin should more prominently declare in the forthcoming NSS that it holds offensive cyber capabilities and that it will use them in accordance with international law. Germany's offensive cyber operations should be conducted only as a response to malicious activity and to halt disruptive operations.[26] Germany should refrain from planting logic bombs in adversaries' critical infrastructure unless direct hostilities exist or are imminent.[27] This would not preclude it from entering adversary networks to gain intelligence and conduct reconnaissance. Germany's capacity to deploy offensive cyber capabilities may spark skepticism, but the Bundeswehr, in 2016, hacked into Afghanistan's cellular network infrastructure to gather information on a hostage incident.[28]

As a reliable cyber power, Germany should share offensive cyber capabilities with trusted EU and NATO members or partners further abroad, if requested, in crisis situations. Bilateral and multilateral agreements would ensure that capabilities are shared only with countries that conduct cyber operations in accordance with international law. Such agreements would also define the capabilities to be shared and the circumstances under which sharing would occur.[29]

Germany's approach to deploying limited offensive cyber capabilities would be in stark contrast to US cyber activities, which hit enemy infrastructure, even that which is related to daily operations,[30] in an effort to degrade an adversary's ability to attack.[31] The United States' current approach relies on its early 21st century war on terrorism, in which eliminating terrorists was common practice. But those

21 Valentin Weber, "Linking Cyber Strategy with Grand Strategy: The Case of the United States," *Journal of Cyber Policy,* August 17, 2018.

22 Bundeswehr, "Luftpatrouillen über Polen und Rumänien" [Air Patrols Over Poland and Romania], March 2, 2022: <https://www.bundeswehr.de/de/organisation/luftwaffe/aktuelles/luftpatrouillen-ueber-polen-und-rumaenien-5364382> (accessed September 30, 2022).

23 Fjori Sinoruka and Vladimir Karaj, "New Cyber-Attacks on Albania Cause Border Chaos," *Balkan Insight* (blog), September 12, 2022: <https://balkaninsight.com/2022/09/12/new-cyber-attacks-on-albania-cause-border-chaos/> (accessed September 30, 2022).

24 Mariam Baksh, "White House Attributes Attack on Albania's Critical Infrastructure to Iran," *Nextgov*, September 7, 2022: <https://www.nextgov.com/cybersecurity/2022/09/white-house-attributes-attack-albanias-critical-infrastructure-iran/376800/> (accessed September 30, 2022).

25 U.S. Cyber Command, "US, Montenegro Work Together to Defend Against Malicious Cyber Actors," October 30, 2019: <https://www.cybercom.mil/Media/News/News-Display/Article/2002939/us-montenegro-work-together-to-defend-against-malicious-cyber-actors/https%3A%2F%2Fwww.cybercom.mil%2FMedia%2FNews%2FArticle%2F2002939%2Fus-montenegro-work-together-to-defend-against-malicious-cyber-actors%2F> (accessed September 30, 2022).

26 Brunner, Schweighofer, and Zanol, "Malicious Cyber Operations, 'Hackbacks' and International Law: An Austrian Example as a Basis for Discussion on Permissible Responses."

27 David E. Sanger and Nicole Perlroth, "U.S. Escalates Online Attacks on Russia's Power Grid," *The New York Times,* June 15, 2019: <https://www.nytimes.com/2019/06/15/us/politics/trump-cyber-russia-grid.html> (accessed September 30, 2022).

28 Matthias Gebauer, "Bundeswehr: Hacker knackten Mobilfunknetz in Afghanistan" [Bundeswehr: Hackers Crack Cell Phone Network in Afghanistan], *Der Spiegel*, September 23, 2016: <https://www.spiegel.de/politik/ausland/cyber-einheit-bundeswehr-hackte-afghanisches-mobilfunknetz-a-1113560.html> (accessed September 30, 2022).

29 Jan Kallberg, Todd Arnold, and Stephen S. Hamilton, "Sharing Cyber Capabilities Within the Alliance - Interoperability Through Structured Pre-Authorization Cyber," West Point Research Papers (Summer 2022): <https://digitalcommons.usmalibrary.org/cgi/viewcontent.cgi?article=1707&context=usma_research_papers> (accessed September 30, 2022).

30 U.S. Cyber Command, "Achieve and Maintain Cyberspace Superiority: Command Vision for US Cyber Command."

31 Michael P. Fischerkeller, Emily O. Goldman, and Richard J. Harknett, "Persistent Engagement in Cyberspace Is a Strategic Imperative," *The National Interest,* July 6, 2022: <https://nationalinterest.org/blog/techland-when-great-power-competition-meets-digital-world/persistent-engagement-cyberspace> (accessed October 1, 2022).

tactical strikes are unlikely to have made the world safer.[32] Crippling an enemy's cyberattack infrastructure may be similarly ineffective. Blocking a Russian propaganda outlet's internet access during midterm elections would impose costs also on US operators whose resources may be better spent building domestic cyber resilience or conducting strategic cyber operations with more lasting effects.[33] US tactical day-to-day operations, around which persistent engagement is built, may have limited long-term value, even cumulatively. This is the case for most Russian cyber operations, too.

Finally, Germany should further enhance its position as a cyber capacity-building actor worldwide, thereby cementing its role as a reliable cyber power. Berlin is already engaged in several cyber capacity-building initiatives, but this engagement should be enlarged and made an integral part of the German strategic narrative.

32 Brian Michael Jenkins, "Five Years After the Death of Osama Bin Laden, Is the World Safer?," *The Rand Blog*, May 2, 2016: <https://www.rand.org/blog/2016/05/five-years-after-the-death-of-osama-bin-laden-is-the.html> (accessed September 30, 2022).

33 Ellen Nakashima, "U.S. Cyber Command Operation Disrupted Internet Access of Russian Troll Factory on Day of 2018 Midterms," *The Washington Post*, February 27, 2019: <https://www.washingtonpost.com/world/national-security/us-cyber-command-operation-disrupted-internet-access-of-russian-troll-factory-on-day-of-2018-midterms/2019/02/26/1827fc9e-36d6-11e9-af5b-b51b7ff322e9_story.html> (accessed September 30, 2022).

DGAP

Advancing foreign policy. Since 1955.

Rauchstraße 17/18
10787 Berlin
Tel. +49 30 254231-0
info@dgap.org
www.dgap.org
@dgapev

The German Council on Foreign Relations (DGAP) is committed to fostering impactful foreign and security policy on a German and European level that promotes democracy, peace, and the rule of law. It is nonpartisan and nonprofit. The opinions expressed in this publication are those of the author(s) and do not necessarily reflect the views of the German Council on Foreign Relations (DGAP).

DGAP receives funding from the German Federal Foreign Office based on a resolution of the German Bundestag.

Publisher
Deutsche Gesellschaft für
Auswärtige Politik e.V.

ISSN 2198-5936

Editing Andrew Cohen

Layout Lara Bührer

Design Concept WeDo

Author picture(s) © Johan Jeansson