INTERNATIONAL ENCRYPTION BRIEF

CARNEGIE
ENDOWMENT FOR
INTERNATIONAL PEACE

PRINCETON
UNIVERSITY

CITP
CENTER FOR
INFORMATION TECHNOLOGY POLICY

MARCH 2021

The Encryption Debate in Germany: 2021 Update

Sven Herpig and Julia Schuetze

© 2021 Carnegie Endowment for International Peace. All rights reserved.

Carnegie does not take institutional positions on public policy issues; the views represented herein are those of the author(s) and do not necessarily reflect the views of Carnegie, its staff, or its trustees.

No part of this publication may be reproduced or transmitted in any form or by any means without permission in writing from the Carnegie Endowment for International Peace. Please direct inquiries to:

Carnegie Endowment for International Peace
Publications Department
1779 Massachusetts Avenue NW
Washington, DC 20036
P: + 1 202 483 7600
F: + 1 202 483 1840
CarnegieEndowment.org

This publication can be downloaded at no cost at CarnegieEndowment.org.

Introduction

Germany's government has supported widespread, strong, and unregulated encryption. In 2014, the government reaffirmed and extended this political commitment when it announced its goal to become the global leader in adopting encryption. Instead of focusing on regulating encryption itself, Germany has worked to enable its security agencies to conduct targeted remote hacking operations. It has even passed a legal framework for that purpose. The legal debate about government hacking authority eventually led to a landmark Federal Constitutional Court ruling emphasizing the government's responsibility for the integrity of information technology systems.[1] While two years ago it seemed highly unlikely that Germany would steer away from its course of supporting strong, secure encryption without lawful access mechanisms,[2] things have changed since then. Germany is exploring lawful access mechanisms on the European level while simultaneously extending government hacking powers in Germany.

While recent revelations about a past agreement between Germany's Foreign Intelligence Agency and the CIA—in which they sold encryption machines with backdoors worldwide through the Crypto AG company[3]—seems to suggest differently, Germany's encryption policy has been clear and consistent for decades. Since 1999, the government has supported widespread strong encryption but has also reserved the right to find solutions for law enforcement and intelligence agencies to access digital evidence through government hacking.[4] Government hacking is understood as "[remotely] interfering with the integrity of software – including online services – or hardware to access data in transit, data at rest, and sensors to manipulate a target's device by law enforcement for the purpose of criminal investigations [in a targeted manner]."[5] Recent incidents, policy and legal developments, and institutional change over the last year did not significantly deviate from Germany's long-standing encryption policy to eschew weakening encryption and rather focus on government hacking on the national level.

However, three policy developments show that Germany's commitment to secure encryption is not as strong anymore as it was before. Firstly, in 2019, state ministries of the interior discussed the possibility of forcing vendors to create backdoors in their messenger applications. This idea was immediately met with strong public criticism that culminated in an open letter to the government against those plans. Within a few days, the letter had been signed by more than 200 companies, organizations, and representatives from academia, civil society as well as members of parliament.[6] Secondly, Germany introduced a resolution on "security through encryption and security despite encryption" under its European Council presidency. The resolution that was adopted in December 2020 supports the development of a regulatory framework and dialogue on solutions that enable competent authorities to "access data in a lawful and targeted manner."[7] While this may just be aiming at implementing a government hacking framework on the European level, it may also aim at lawful access mechanisms. Lastly, the German Federal Foreign Office published a non-paper on EU cyber diplomacy together with Estonia, France, Poland, Portugal, and Slovenia.[8] A single sentence revealed Germany's deteriorating support for strong and secure encryption: "The EU and its Member States are invited to find solutions that allow law enforcement and other competent authorities to gain lawful access to digital evidence concerning malicious cyber activities, without prohibiting or *generally* weakening encryption, and in full respect of privacy and fair trial guarantees consistent with applicable law [emphasis added]."

Key Actors Development

Germany has made progress at the institutional level with two new agencies to contribute to the growing landscape of German government cybersecurity-related institutions. The Central Office for Information Technology in the Security Sector (ZITiS) was founded in 2017 but the hiring process and consequently the setup of the agency has taken time. The agency—which is supposed to offer procurement and training in, among other things, government hacking tools—seems to be fully operational now and its resources and authorities are to be extended.[9]

Most recently, in August 2020, the Innovation Agency for Cybersecurity, sometimes called the German DARPA, after the U.S. Defense Advanced Research Projects Agency, was launched under joint auspices of the Ministry of the Interior, Building and Community and the Ministry of Defense.[10][11] It is tasked with fostering research regarding technological sovereignty and security. While there has not been a definitive announcement yet, it is likely that the agency will also cover projects that deal with government hacking, encryption, and lawful access.

FinFisher

Netzpolitik.org, a German language blog on digital rights, published a classified response to a written parliamentary inquiry that states that the FinFisher company provides government-grade commercial surveillance spyware sold exclusively to government agencies for use in targeted and lawful criminal investigations. The company has its Germany-based branch, Gamma International GmbH, in Munich, the same location as ZITiS. The company, which is known to work together with the Federal Office for Criminal Investigations (BKA), the German agency with the product FinSpy,[12] is being investigated for possible violations of the Foreign Trade Act by exporting powerful spying software without a permit. The Ministry of Economy said the government had not issued any export permits for spying software since 2015.[13] Nongovernmental organizations—the Society for Civil Rights, Reporters Without Borders e.V., the European Center for Constitutional and Human Rights and Netzpolitik.org—filed a complaint against FinFisher after IT security experts from the Chaos Computer Club showed how its software matched software used to spy on Turkish opposition protesters.[14] The criminal complaint against FinFisher caused the Munich public prosecutor's office to search the company's business premises and private apartments of people who work at the company in October 2020. The outcome of the investigation is pending.[15]

Tech Companies

Tech companies, especially internet service providers, have been vocal when it comes to the use of government hacking tools. Led by the Association of the Internet Industry, internet service providers criticize the fact that the federal government is increasingly deputizing them for their government hacking operations.[16] While currently internet service providers only have to give security agencies access to their facilities and forward information, pending laws would allow government agencies to mandate that service providers: force software updates and security software on their customers' devices,[17] and deliver government surveillance software to their targets directly.[18]

Related Issues Development

Encryption Workaround for WhatsApp

In July 2020, news broke that the Federal Criminal Police Office—an agency known for creative encryption workarounds—was circumventing encryption in the popular messaging platform WhatsApp.[19] The method used in this particular case is far from exciting. Law enforcement got physical access to the devices, enabled the "WhatsApp Web" feature connecting it to the law enforcement staff's browser, and then returned the devices to the suspects. It remains unclear whether the devices were passcode-protected and whether the suspects were aware that their device had been tampered with. While potentially successful, the approach is resource intensive and prone to errors. The agency needs physical access to the device—without the suspect noticing—and to break any existing passcode. On the other hand, the compromise can be easily spotted if the target checks their open WhatsApp Web sessions on the phone. This incident, though technically not very sophisticated, is worth mentioning as it highlights once again the government's approach toward hacking and encryption workarounds. The action is not without precedent; in 2017, it was reported that the agency was able to apply an encryption workaround to bypass security protocols on the Telegram messenger app.[20]

Usage of Government Hacking

The scope of government hacking operations remained mostly unclear up until 2021, when the Federal Ministry of Justice published data on the use of government hacking operations in their statistics for the first time.[21] According to this new information, the police and investigative authorities ordered the more invasive online search thirty-three times in twenty-one procedures and actually used it in twelve cases.[22] Source telecommunications surveillance (that is, hacking to eavesdrop on ongoing communications) was ordered thirty-one times and actually used in three cases.[23] These authorities use government hacking tools primarily to investigate drug and property crimes, not murder or terrorism as initially intended.[24] Another report states that government hacking tools have not been used by the BKA in any successful criminal investigation or emergency response between 2017 and 2020.[25] The president of the BKA confirmed that the current government hacking tools are of use only in a limited number of targeted operations and require vulnerabilities to exploit.[26] Nevertheless, the usage of government hacking is being expanded.

Expansion of government hacking powers in the state level police legislations

German states are reforming their police laws to expand surveillance capabilities following legislation passed by the federal parliament in 2017, which intensified the use of government hacking for law enforcement.[27] The expansion of powers arrives amid an overall decrease in crime rates but an increase in those specific crimes: illegal distribution of pornographic material online, computer-related crimes, children sexual abuse material, resistance to and assault on state power, and offenses under the Medicines Act.[28]

From 2017 to 2020, source telecommunications monitoring has been made legal in seven out of sixteen states (Baden-Wurttemberg, Bavaria, Hesse, North Rhine-Westphalia, Rhineland-Palatinate, Lower Saxony, and Mecklenburg-Western Pomerania) and is currently being discussed in Saarland.[29] The use of all government hacking methods by police was included in four out of sixteen states (Bavaria, Hesse, Rhineland-Palatinate, and Lower Saxony). The police legislation reforms were passed by different coalitions of parties including the Christian Democrats, Social Democrats, Liberals, and Alliance 90/The Greens. In Brandenburg, The Left party blocked an inclusion to other police reforms of government hacking powers in situations of imminent danger in 2019.[30] It remains to be seen whether the new legislation will be permanent. Both state and federal legislations are subject to several pending constitutional complaints.[31] The constitutional court's determination on the federal legislation is the most consequential as any changes at the federal level would necessitate reforms of state-level legislation as well.

Expansion of government hacking policies

Another package of legal amendments, the Law for the Harmonization of Intelligence Laws, if passed, would grant all German intelligence agencies, including all those on the state-level, the power to conduct government hacking operations. One of these amendments would further require service providers to facilitate compromising target devices with government malware.[32] While initially the law was supposed to allow intelligence agencies to access data and communications obtained after the device is wiretapped through surveillance software (called *Quellen-TKÜ*) as well as already existing data and communication on the device (called *Online Durchsuchung*),[33] negotiations would currently only allow them to access data and communication from the date that the warrant was signed (called *Quellen-TKÜ Plus*).[34]

The current draft of yet another pending security amendment, an update of the Federal Policy Law, currently stipulates that the Federal Police shall be given the power to conduct government hacking operations as a preventive measure—in cases where no crime has been committed yet.[35] This would be unchartered territory for the German government hacking framework as so far it has only covered the investigation of crimes.

Vulnerabilities Management

There has been no breakthrough on negotiations over a German vulnerabilities equities process,[36] an essential process for balancing information technology and cybersecurity with government hacking operations. While internal concepts exist and are discussed, the ministry in charge was not yet able to have all involved parties agree to a consensus.

However, there are relevant legal amendments pending to be discussed by the parliament (as of March 2021) regarding government hacking and encryption policy. The leading package of legal amendments, dubbed the Second Law for the Improvement of Security for Information Systems, includes provisions regarding the management of vulnerabilities.[37] Unfortunately, the specific part is so confusing that without the much needed vulnerabilities equities process, it is not entirely clear what it would mean for government hacking operations.[38] The management of vulnerabilities may become even more contentious as another amendment in the Second Law for the Improvement of Security for Information Systems would make the Federal Office for Information Security (BSI) responsible for digital consumer protection, giving the agency rights to analyze software and inquire about all kinds of information from vendors and manufacturers. So, while on the one hand the agency will be responsible to find more vulnerabilities and protect consumers in the cyber domain, the overall governmental vulnerability management is hardly regulated.

Conclusion and Outlook

While there will always be a small group within German government and security circles who believes that weakening encryption will enable intelligence and law enforcement agencies to be more effective without sacrificing IT- and cybersecurity, this group's impact has been negligible until 2020. Public debates in the aftermath of violent events about extending the powers of law enforcement and intelligence agencies in cyberspace are limited to government hacking, not backdoors.[39] From operational, institutional, policy, and legal views, Germany continues to adhere to the encryption policy it adopted in 1999: fostering strong encryption but enabling its intelligence and law enforcement agencies to conduct government hacking, at least on the national level. With its proposed EU council resolution and EU cyber diplomacy non-paper, Germany currently seems to be moving the backdoor and lawful access debate to the EU level—possibly because it knows its chances to pass these policies on the national level are very slim. Whether the EU will be an easier vector to broach these policies remains to be seen.

About the Authors

Sven Herpig is head of international cybersecurity policy at the Berlin-based think tank Stiftung Neue Verantwortung.

Julia Schuetze is junior project director of international cybersecurity policy at the Berlin-based think tank Stiftung Neue Verantwortung.

About the Encryption Working Group

The Carnegie Endowment for International Peace and Princeton University have convened a small group of experts to advance a more constructive dialogue on encryption policy. The working group consists of former government officials, business representatives, privacy and civil rights advocates, law enforcement experts, and computer scientists. Observers from U.S. federal government agencies attended a select number of working group sessions. Since 2018, the working group has met to discuss a number of important issues related to encryption policy, including how the relevant technologies and uses of encryption will evolve in the future.

This brief and its companion pieces detailing the encryption debates in a select number of key countries and regions—Australia, Brazil, China, the European Union, Germany, and India—were prepared by local and area experts at the request of the Encryption Working Group. They are designed to shine light on key drivers of the debates in these countries, how they have evolved in the last five years, and the divergent approaches taken by different governments. The briefs do not take a position on encryption policy, rather they provide analysis of how debates about encryption have evolved internationally. The views are the authors' own and do not necessarily reflect the views of Carnegie or the Encryption Working Group.

Notes

[1] "Leitsätze zum Urteil des Ersten Senats vom 27. Februar 2008 - 1 BvR 370/07 - - 1 BvR 595/07" [in German], German Federal Constitutional Court, accessed March 12, 2021, https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2008/02/rs20080227_1bvr037007.html.

[2] Sven Herpig and Stefan Heumann, "The Encryption Debate in Germany," Carnegie Endowment for International Peace, May 30, 2019, https://carnegieendowment.org/2019/05/30/encryption-debate-in-germany-pub-79215.

[3] Greg Miller, "The Intelligence Coup of the Century," *Washington Post*, February 11, 2020, https://www.washingtonpost.com/graphics/2020/world/national-security/cia-crypto-encryption-machines-espionage/?itid=hp_ed-picks_crypto211%3Ahomepage%2Fstory-ans.

[4] Herpig and Heumann, "The Encryption Debate in Germany."

[5] Sven Herpig, "A Framework for Government Hacking in Criminal Investigations," Stiftung Neue Verantwortung, October 2018, https://www.stiftung-nv.de/sites/default/files/framework_for_government_hacking_in_criminal_investigations.pdf.

[6] "Open Letter to the German Federal Ministry of the Interior, Building and Community," June 11, 2019, accessed March 12, 2021, https://docs.zoho.com/file/eykeu5682e11c122046debcc3f0e6e16c4e13.

[7] "Encryption: Council Adopts Resolution on Security Through Encryption and Security Despite Encryption," Council of the European Union, December 14, 2020, https://www.consilium.europa.eu/en/press/press-releases/2020/12/14/encryption-council-adopts-resolution-on-security-through-encryption-and-security-despite-encryption/.

[8] "Non-Paper on EU Cyber Diplomacy by Estonia, France, Germany, Poland, Portugal and Slovenia," German Ministry of Foreign Affairs, 2019, https://www.auswaertiges-amt.de/blob/2418160/206b3bf9aa4ef45a2887399231840d23/201119-non-paper-pdf-data.pdf.

[9] "Innovativ, vernetzt, verantwortungsvoll" [in German], *Behörden Spiegel*, August 2020, https://issuu.com/behoerden_spiegel/docs/2020_august; and Konstantin von Notz, "Antworten der Bundesregierung zeigen: Zentrale Fragen zu Staatstrojanern, zum staatlichen Handel mit Sicherheitslücken, ZITIS & Co. unbeantwortet" [in German], Grün Digital, February 21, 2021, https://gruen-digital.de/2021/02/antworten-der-bundesregierung-zeigen-zentrale-fragen-zu-staatstrojanern-zum-staatlichen-handel-mit-sicherheitsluecken-zitis-co-unbeantwortet/.

[10] Wim Orth, "Innovationsagentur für Cyber-Sicherheit gegründet" [in German], *Behörden Spiegel*, August 11, 2020, https://www.behoerden-spiegel.de/2020/08/11/innovationsagentur-fuer-cyber-sicherheit-gegruendet/.

[11] Julia Schuetze, "'German DARPA' to Be Established," Stiftung Neue Verantwortung, September 3, 2018, https://www.stiftung-nv.de/de/publikation/transatlantic-cyber-forum-policy-debates#September.

[12] Andre Meister, "Das Bundeskriminalamt kann jetzt drei Staatstrojaner einsetzen" [in German], Netzpolitik.org, June 26, 2018, https://netzpolitik.org/2018/geheime-dokumente-das-bundeskriminalamt-kann-jetzt-drei-staatstrojaner-einsetzen/#vorschaltbanner.

[13] Samantha Early, "German Prosecutors Investigate Spyware Maker FinFisher," Deutsche Welle, September 5, 2019, https://www.dw.com/en/german-prosecutors-investigate-spyware-maker-finfisher/a-50293812.

[14] Ibid.

[15] Daniela Turß, "Pressemitteilung: GFF-Strafanzeige trägt Früchte – Durchsuchung bei Münchener Firma FinFisher wegen Exports von Staatstrojanern" [in German], Gesellschaft für Freiheitsrechte, October 14, 2020, https://freiheitsrechte.org/pm-finfisher-durchsuchung/.

16 “Stellungnahme zum Entwurf eines Gesetzes zur Anpassung des Verfassungsschutzrechts” [in German], Eco, Verband der Internetwirtschaft e.V., June 30, 2020, https://www.eco.de/download/127303/; and Patrick Beuth, “Firmen sollen Geheimdiensten beim Installieren von Staatstrojanern helfen” [in German], *Der Spiegel*, July 7, 2020, https://www.spiegel.de/netzwelt/netzpolitik/verfassungsschutzreform-firmen-sollen-beim-installieren-von-staatstrojanern-helfen-a-8fd775f1-f3f6-42f4-a9bb-c1c36b2afb8b.

17 Sven Herpig and Jan-Peter Kleinhans, “Stellungnahme zum Referentenentwurf ‘IT-Sicherheitsgesetz 2.0’ – in der Fassung vom 09.12.2020 – des Bundesministeriums des Innern, für Bau und Heimat” [in German], Stiftung Neue Verantwortung, December 9, 2020, https://www.stiftung-nv.de/sites/default/files/snv_-_stellungnahme_-_it-sig_2.0_-_9_dezember_2020_0.pdf.

18 Kilian Vieth et al., “Stellungnahme zum Referentenentwurf des Bundesministeriums des Innern, für Bau und Heimat ‘Entwurf eines Gesetzes zur Anpassung des Verfassungsschutzrechts’” [in German], Stiftung Neue Verantwortung, June 13, 2020, https://www.stiftung-nv.de/sites/default/files/snv_stellungnahme_bverfschg-g10_entwurf_13062020.pdf.

19 Florian Flade and Hakan Tanriverdi, “BKA kann bei WhatsApp mitlesen” [in German], tagesschau.de, July 21, 2020, https://www.tagesschau.de/inland/bka-whatsapp-101.html.

20 Sven Herpig, “Government Hacking: Computer Security vs. Investigative Powers,” Stiftung Neue Verantwortung, June 2017, https://www.stiftung-nv.de/sites/default/files/snv_tcf_government_hacking-problem_analysis_0.pdf.

21 “Übersicht Online-Durchsuchung 2019” [in German], German Federal Office of Justice, February 19, 2020, accessed March 12, 2021, https://www.bundesjustizamt.de/DE/SharedDocs/Publikationen/Justizstatistik/Uebersicht_Online_Durchsuchung_2019.html?__blob=publicationFile%22%3E12.

22 See under facts differentiation between online search and source communication surveillance: Julia Schuetze, “Intensification of Targeted Surveillance of Suspects Via So Called ‘State Trojan’ Software,” Stiftung Neue Verantwortung, June 27, 2017, https://www.stiftung-nv.de/de/publikation/transatlantic-cyber-forum-policy-debates#%E2%80%9DJune. And: “Übersicht Online-Durchsuchung 2019” [in German], German Federal Office of Justice, February 19, 2020, accessed March 12, 2021, https://www.bundesjustizamt.de/DE/SharedDocs/Publikationen/Justizstatistik/Uebersicht_Online_Durchsuchung_2019.html?__blob=publicationFile%22%3E12.

23 “Übersicht Telekommunikationsüberwachung 2019” [in German], German Federal Office of Justice, last modified February 12, 2020, accessed March 12, 2021, https://www.bundesjustizamt.de/DE/SharedDocs/Publikationen/Justizstatistik/Uebersicht_TKUE_2019.pdf?__blob=publicationFile&v=7.

24 Andre Meister, “Polizei nutzt Staatstrojaner vor allem bei Erpressung und Drogen” [in German], Netzpolitik.org, Feb. 18, 2021, https://netzpolitik.org/2021/justizstatistik-2019-polizei-nutzt-staatstrojaner-vor-allem-bei-erpressung-und-drogen/.

25 von Notz, “Antworten der Bundesregierung zeigen.”

26 Holger Münch, “BKA-Präsident Münch im Interview: ‘In der Pandemie rüstet die Polizei digital auf’” [in German], interview by Hans-Jürgen Degelow, Heilbronner Stimme, January 23, 2021, https://www.bka.de/DE/Presse/Interviews/2021/210123_InterviewMuenchHeilbronnerStimme.html.

27 Schuetze, “Intensification of Targeted Surveillance of Suspects Via So Called ‘State Trojan’ Software.”

28 “Polizeiliche Kriminalstatistik 2019 Ausgewählte Zahlen im Überblick” [in German], German Federal Ministry of the Interior, Building and Community, 2019, accessed March 12, 2021, https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/sicherheit/pks-2019.pdf?__blob=publicationFile&v=10#:~:text=Betrachtet%20man%20die%20%E2%80%9EStraftaten%20insgesamt,ist%20dies%20der%20niedrigste%20Stand.

[29] Markus Drescher, “Trojaner erreichen den Nordosten” [in German], Neues Deutschland, March 3, 2020, https://www.neues-deutschland.de/artikel/1134165.neue-polizeigesetze-trojaner-erreichen-den-nordosten.html; and “Übersicht über die Änderungen der Polizeigesetze in den einzelnen Bundesländern” [in German], Amnesty International and Gesellschaft für Freiheitsrechte, last modified April 18, 2019, accessed March 12, 2021, https://www.amnesty.de/sites/default/files/2019-04/Uebersicht-ueber-die-Aenderungen-der-Polizeigesetze-in-den-einzelnen-Bundeslaendern-Maerz2019_0.pdf.

[30] Marie Bröckling, “Staatstrojaner verhindert, Grundrechte trotzdem beschnitten” [in German], Netzpolitik.org, March 14, 2019, https://netzpolitik.org/2019/brandenburger-polizeigesetz-staatstrojaner-verhindert-grundrechte-trotzdem-beschnitten/#vorschaltbanne.

[31] Nora Markard, “GFF erhebt Verfassungbeschwerde gegen massenhaften Einsatz von ‘Staatstrojanern’” [in German] Gesellschaft für Freiheitsrechte, May 20, 2017, https://freiheitsrechte.org/trojaner/; Stefan Krempl, “Bundestrojaner & Co.: Neue Verfassungsbeschwerde gegen das BKA-Gesetz” [in German], heise online, September 4, 2019, https://www.heise.de/newsticker/meldung/Bundestrojaner-Co-Neue-Verfassungsbeschwerde-gegen-das-BKA-Gesetz-4513244.html; and “’Hessentrojaner’ beim BVerfG” [in German], Legal Tribune Online, July 3, 2019, https://www.lto.de/recht/nachrichten/n/hessen-verfassungsbeschwerde-polizeigesetz-online-durchsuchungen-trojaner-persoenlichkeitsrecht-profile/.

[32] Vieth, “Stellungnahme zum Referentenentwurf des Bundesministeriums des Innern, für Bau und Heimat ‘Entwurf eines Gesetzes zur Anpassung des Verfassungsschutzrechts’.”

[33] For an explanation of German government hacking categories, see Schuetze, “Intensification of Targeted Surveillance of Suspects Via So Called ‘State Trojan’ Software.”

[34] Ronen Steinke, “Vom Trojaner zum Trojaner plus” [in German], *Süddeutsche Zeitung*, August 19, 2020, https://www.sueddeutsche.de/digital/staatstrojaner-quellen-tkue-verfassungsschutz-1.5001279.

[35] Andre Meister, “Große Koalition will Staatstrojaner gegen Personen einsetzen, die noch keine Straftat begangen haben” [in German], Netpolitik.org, February 17, 2021, https://netzpolitik.org/2021/bundespolizeigesetz-grosse-koalition-will-staatstrojaner-gegen-personen-einsetzen-die-noch-keine-straftat-begangen-haben/.

[36] Sven Herpig, “German Vulnerabilities Equities Process,” Stiftung Neue Verantwortung, June 8, 2018, https://www.stiftung-nv.de/de/publikation/transatlantic-cyber-forum-policy-debates#%E2%80%9DJune8%E2%80%9D.

[37] Herpig, and Kleinhans, “Stellungnahme zum Referentenentwurf ‘IT-Sicherheitsgesetz 2.0’ – in der Fassung vom 09.12.2020 – des Bundesministeriums des Innern, für Bau und Heimat.”

[38] Ibid.

[39] See for example: Ulf Buermeyer and Sven Herpig, “Immer neue Sicherheitsgesetze helfen nicht” [in German], zeit online, Oct. 14, 2019, https://www.zeit.de/politik/deutschland/2019-10/anschlag-halle-rechtsterrorismus-sicherheitsgesetze-moratoriu.

CARNEGIE
ENDOWMENT FOR
INTERNATIONAL PEACE

1779 Massachusetts Avenue NW | Washington, DC 20036 | P: + 1 202 483 7600

CarnegieEndowment.org