INTERNATIONAL ENCRYPTION BRIEF

MAY 2019

The Encryption Debate in Germany

Sven Herpig and Stefan Heumann

The Encryption Debate in Germany

Sven Herpig and Stefan Heumann

For your convenience, this document contains hyperlinked source notes as indicated by teal colored text.

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.

CONTENTS

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 briefing paper 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.

The Encryption Working Group will continue its efforts to study this important issue and plans on releasing further briefings on aspects of the encryption policy debate.

Members of the Encryption Working Group include:

Jim Baker
Former General Counsel, Federal Bureau of Investigation

Katherine Charlet
Program Director, Technology and International Affairs, Carnegie Endowment for International Peace

Tom Donahue
Visiting Fellow, George Mason National Security Institute, and former Senior Director for Cyber Operations, National Security Council, White House

Ed Felten
Robert E. Kahn Professor of Computer Science and Public Affairs, Princeton University

Avril Haines
Senior Research Scholar at Columbia University's Columbia World Projects and former Deputy Director, Central Intelligence Agency

Susan Hennessey
Executive Editor, Lawfare, and Senior Fellow in Governance Studies, the Brookings Institution

Chris Inglis
Managing Director, Paladin Capital Group, and former Deputy Director, National Security Agency

Sean Joyce
US Cybersecurity and Privacy Leader, PwC, and former Deputy Director, Federal Bureau of Investigation

Susan Landau
Bridge Professor of Cyber Security and Policy, Tufts University

Christy Lopez
Distinguished Visitor from Practice, Georgetown Law Center

Alex Macgillivray
Board Member, Data & Society, and former Deputy Chief Technology Officer of the United States

Jason Matheny
Founding Director, Georgetown Center for Security and Emerging Technology, and former Director, Intelligence Advanced Research Projects Activity

Tim Maurer
Co-Director and Fellow, Cyber Policy Initiative, Carnegie Endowment for International Peace

Denis McDonough
Visiting Senior Fellow, Technology and International Affairs, Carnegie Endowment for International Peace, and former White House Chief of Staff

Lisa Monaco
Distinguished Senior Fellow, Reiss Center on Law and Security, New York University School of Law, and former Assistant to the President for Homeland Security and Counterterrorism

Laura Moy
Executive Director, Center on Privacy & Technology, Georgetown Law Center

Michelle Richardson
Director, Privacy and Data Project, Center for Democracy and Technology

Ronald L. Rivest
Institute Professor, Massachusetts Institute of Technology

Ari Schwartz
Managing Director of Cybersecurity Services, Venable LLP

Harlan Yu
Executive Director, Upturn

Denise Zheng
Senior Associate (Non-resident), Technology Policy Program, Center for Strategic and International Studies

Note: This is not a comprehensive list of all members. Some wish to remain anonymous for the time being and to contribute in their personal capacity.

Since 1999, Germany's government has strongly 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. However, the government has simultaneously reserved the right to respond appropriately when encryption technology severely limits the ability of law enforcement and intelligence agencies to do their jobs. Instead of focusing on regulating encryption itself, Germany has worked to enable its security agencies to conduct hacking. It has even passed a legal framework tailored to government hacking operations. Civil society and industry representatives have mounted legal challenges against the corresponding provisions. The legal debate eventually led to a landmark supreme court ruling emphasizing the government's responsibility for the integrity of information technology systems. The conversation is far from over, with some supreme court cases still pending in regard to recent legislation on the lawful hacking framework.

Introduction

In its Digital Agenda 2014–2017, the German government explicitly outlined its goal for Germany to become "the world's leading country" in adopting encryption. This goal builds on Germany's first policy on encryption,[1] loosely translated as the "crypto principles," which the government announced in 1999.[2] Senior officials have repeatedly affirmed—most recently in 2017—the validity of this policy. In summary, the five core elements are:

1. There will be no ban or limitation on [encryption] products.
2. [Encryption] products shall be tested for their security in order to increase the user's trust in those products.
3. The development of [encryption] products by German manufacturers is essential for the country's security and [for those companies'] ability to compete internationally, and shall therefore be strengthened.
4. Law enforcement and security agencies shall not be weakened by the widespread use of encryption. The development of additional technical competencies for those agencies shall be fostered.
5. International cooperation on [encryption] issues such as open standards and interoperability is vital and shall be fostered bi- and multilaterally.

Two aspects that are in direct opposition to each other are the government's position that there will be no limitation on the free availability of encryption products, and that law enforcement and security agencies should be able to do their jobs despite the widespread application and use of encryption. So far, the government has been able to deliver on both accounts: it has neither weakened nor regulated encryption, and law enforcement still appears able to do its job.

Background

Separating Code Making and Code Breaking

The earliest aspects of Germany's current stance on encryption policy can be traced back to the establishment of its national cybersecurity agency, the Federal Office for Information Security (BSI). With the BSI's creation in 1991, Germany formally separated code making from code breaking, which until then had been consolidated in the Federal Intelligence Service. While the Federal Intelligence Service directly reports to the chancellery, BSI is under the supervision of the Ministry of the Interior, Building, and Community. This separation is quite substantial from a bureaucratic perspective and puts encryption policy entirely in the civilian domain. The segregation of code making and code breaking is still in effect. However, the BSI as code maker and several other agencies that serve as code breakers (namely the domestic intelligence agency, the Federal Office for Criminal Investigation, and the Central Office for Information Technology in the Security Sector), are all under the supervision of the same ministry. In recent years, the political climate appears to have cemented this separation rather than weakened it. Political parties as well as representatives from private sector, academia, and especially civil society have advocated for stronger—or even complete—independence of the BSI from the Ministry of the Interior, Building, and Community for that very reason.

2008 Supreme Court Ruling

Instead of weakening encryption or mandating backdoors, Germany decided to focus on enabling its law enforcement and security agencies to engage in lawful hacking. The government's technical and legal developments in the area of lawful hacking led to a case at Germany's highest judicial body, the Federal Constitutional Court. In a landmark 2008 ruling, the court stated that it is the government's responsibility to guarantee the "integrity of information technology systems." The ruling added further safeguards to basic legal protections for private communications. After amendments on lawful hacking were passed in 2017, the court was called upon again—by information technology (IT) industry and civil society—to decide on the validity of the new legal framework. The case is currently pending and will likely be decided in 2019.

Impact of the Snowden Revelations

In 2013, the revelations made by former U.S. intelligence analyst Edward Snowden

> Strengthened the position of those who were worried about the government's commitment to strong encryption. The revelations about global [U.S. National Security Agency] surveillance programs and their potential impact on Germany spurred a debate about the government's responsibility and role to protect data and information infrastructures of German citizens and companies. The necessity to promote and implement strong encryption

> played a prominent role in this debate. When the government . . . published its first digital strategy called [Digital Agenda 2014–2017] in September 2014, it set out the ambitious goal of making Germany the global leader on the adoption of encryption. At the occasion of the national IT summit in 2015, representatives from the IT industry and government officials signed the end-to-end encryption [charter], another pledge for strong encryption.

Key Actors

Germany's encryption debate involves the same set of actors as in many other countries: the intelligence community, law enforcement, policymakers, tech companies, industry, and civil society. But Germany's historical, cultural, and institutional background makes its debate different from that in other countries. Because of unique historical experiences with surveillance during Nazi rule and the East German Communist regime, the German intelligence community does not enjoy the positive public image that those in the United States and the United Kingdom do, and thus usually adopts a very low profile in public debates. As such, law enforcement is usually the most visible government actor in the encryption debates. Yet the German government is far from a monolithic bloc. It also includes the data protection agencies and other agencies and stakeholders that take a strong interest in promoting encryption, such as the Federal Office for Information Security.

Any attempts to regulate encryption to facilitate access to communications and data by law enforcement would meet strong opposition from civil society. The data protection and privacy community is very active in the encryption debate, advocating for the right to privacy of personal communications. Germany is also home to the Chaos Computer Club, the largest association of hackers in Europe and a powerful voice in the country's public debate on IT security and encryption. Members of the organization have frequently exposed security flaws in IT systems and used such stunts to advocate for higher IT security standards, including stronger encryption. But the German activist and advocacy scene extends beyond the club, including journalists from Netzpolitik.org, lawyers at the Society for Civil Rights, members of the Computer Scientists for Peace and Social Responsibility, as well as international outlets like AccessNow and Reporters Without Borders. All of these publicly and politically hold the government responsible for shortcomings related to privacy and cybersecurity policies.

Tech companies are also an important stakeholder in the debate. The most popular platforms and communication service providers are largely based abroad, particularly in the United States. They, too, have usually tried to keep a low profile in this debate. The same is true for German industry. But the growing use and reliance on digital communications and other IT systems has made them much more driven to participate in the debate.

Policymakers do not fall into one specific camp in this debate. The conservative and Social Democratic parties tend to be quite sympathetic to the needs of law enforcement. The Green Party,

Left Party, and Liberal Party have generally been much more critical of any government attempt to regulate encryption and have strongly defended the use of encryption as an important tool to protect the confidentiality of personal communications. However, those are only general tendencies with outliers in each camp.

Overall, the debate in Germany has not centered on the regulation of encryption with regard to any potential backdoors for government access. Instead, the government has embraced lawful hacking as a third way that would allow access for law enforcement and other security purposes without weakening encryption through regulation.

Main Issues

Encryption Policy Developments, 2014–2016

In 2014, the newly formed government under Chancellor Angela Merkel (her third cabinet) agreed on a much-needed action plan to further digitization in Germany, which became the Digital Agenda 2014–2017.[3] The agenda has seven core areas, and the sixth focuses on security and reaffirms Germany's stance on encryption policy. The agenda states its ambitious goal to make Germany the world's leading country in adopting encryption. Yet it is unclear if that goal has been achieved. In 2018, for example, only 13.5 percent of email users reported using end-to-end-encryption.[4] Successful government projects in this field are also rare. While the government tried to roll out a secure and authenticated email service (dubbed De-Mail[5]) for official correspondence, a meaningful rate of adoption was never reached. This was in part attributed to the fact that the first version of De-Mail did not implement true end-to-end encryption. Messages were decrypted and re-encrypted during transport on a secure server in order to check for malware. This did not sit too well with German activists and the public, who interpreted this as an intentional design to spy on their email exchanges.

Encryption Becomes State of the Art

Many recent laws and regulations, such as the e-health law passed in 2015,[6] require secure encryption. The e-health law states that a key requirement for electronic processing of health data is the implementation of appropriate, state-of-the-art technical measures to protect it against unauthorized access.[7] "State-of-the-art technical measures" are widely interpreted as requiring compliance with technical guidelines and other guidance currently offered by the BSI. Therefore, secure encryption (algorithms and implementation without backdoor access or key escrow and the like), as advocated by the BSI, has become the de jure baseline IT security standard for technical measures.

The 2016 Cybersecurity Strategy

Germany's current cybersecurity strategy was published in 2016.[8] One of the few paragraphs with strategic relevance was dedicated to the role of encryption in keeping Germany safe. It equivocally states that the government aims to improve "security through encryption" and "security despite encryption." While the strategy does not rule out weakening encryption through regulation or lawful access mechanisms, it reaffirms the wording from the 1999 principles, which stated that law enforcement and security agencies should not be hindered by widespread encryption.

Another aspect of the strategy worth mentioning is the establishment of a new agency, the Central Office for Information Technology in the Security Sector (ZITiS).[9] The agency is tasked with vulnerability research and acquisition as well as the development and acquisition of hacking tools and services, which it can provide to Germany's law enforcement and intelligence agencies. It is supposed to be a one-stop-shop for state and federal security agencies looking for data access and management tools. This ties in perfectly with the ongoing lawful hacking debate. When it was announced that ZITiS would be established under the same ministry as the BSI, calls for the BSI to have more independence grew louder for fear that it might be forced to cooperate with the new code breaker, for example by supporting it with knowledge of vulnerabilities.

Related Issues

Lawful Hacking

As the Federal Constitutional Court cases show, policymakers, lawyers, researchers, and activists in Germany have been fighting over the legal framework allowing security agencies to conduct hacking operations against criminals in Germany for over a decade.[10] The legal basis, until very recently, has mainly been the Federal Office for Criminal Investigation Law.[11] The parliament passed the latest legal amendment for lawful hacking in 2017,[12] which, as mentioned, has been directly challenged in separate Federal Constitutional Court cases. This conflict has many facets, ranging from its potential violation of the court's ruling on the integrity of information technology systems, to the exact design and limitations of the hacking software used by the agencies.

The government has apparently decided that enabling hacking operations conducted by its security and intelligence agencies, while not meddling with encryption, is its silver bullet for the perceived going dark challenge. The internal restructuring within the Ministry of the Interior stands witness to this development as well. In 2018, the ministry solidified supervision over the BSI and all code-breaking agencies within its newly founded division on cyber and IT security.[13] New teams for the development of cyber capacities for the code breakers have been set up as well, so out of the eight teams in that division, three are tasked with facilitating lawful hacking and similar activities for the security and intelligence agencies.

The Telegram Hack

Going down the lawful hacking road satisfies the promises made in both the 1999 crypto principles and the 2016 cybersecurity strategy. It does not weaken encryption or devices but enables law enforcement and security agencies to do their jobs and collect digital evidence. This approach was showcased by the law enforcement hack of the Telegram messenger app. In 2014, the Federal Office for Criminal Investigation hacked the supposedly secure Telegram accounts of eight users, who were suspects in an ongoing criminal investigation into an extremist right-wing group. This hack allowed the office to access the entire history of unencrypted messages (including media files) connected to the accounts, as well as new messages that arrived in real time since all messages are centrally saved on Telegram's servers. The hack used a mixture of features and flaws in the application and account design.[14]

Establishing a Vulnerabilities Equities Process

Befitting Germany's stance on encryption policy and the subsequent operational need for lawful hacking is its current plan to develop a national vulnerabilities equities process and policy.[15] The Ministry of the Interior, Building, and Community is currently drafting a policy proposal, which it announced during a cybersecurity conference jointly organized by the Federal Academy for Security Policy and the think tank Stiftung Neue Verantwortung in June 2018. In addition to the legal amendments on lawful hacking passed in 2017 and the creation of ZITiS, establishing a vulnerabilities equities process will be yet another piece in Germany's lawful hacking strategy.

Conclusion and Outlook

It is no secret that Germany often prefers regulation to other policies. This also holds true for cybersecurity, as demonstrated by the IT security law implementing protections for critical infrastructure. It was passed in 2015,[16] preceding the EU-wide regulation, the Directive on Security of Network and Information Systems.[17] It is also true, however, that the target of encryption regulation would not be German companies but international, mainly U.S., companies that operate worldwide. Apple, Google, and Facebook do, of course, operate in Germany and have representatives there, but regulating them on encryption might be more difficult than regulating German companies. While the recent adoption of the Act to Improve Enforcement of the Law in Social Networks shows it is possible,[18] there have not been any attempts to weaken encryption or require vendor assistance for lawful access so far.

For a European Union member, encryption regulation might not only be a national issue but could also be elevated to the supranational level. Regulation to leverage the EU's Digital Single Market, such as the General Data Protection Regulation (GDPR),[19] shows that something similar might also

be possible for encryption. Even though there were rumors about a joint French-German approach toward regulating encryption at the EU level in 2017, nothing has come out of it so far. German officials have denied that there was ever the intention to do so.[20]

Since 1999, Germany's principles on encryption policy have not changed. The government takes a clear and unambiguous stance toward strong encryption as a fundamental element for IT security and, hence, the protection of government networks, the economy, and German citizens. While those principles also clearly state that law enforcement and intelligence agencies have to be able to do their jobs, the government has not yet challenged strong encryption. Rarely have German officials publicly voiced their concern about the inaccessibility of evidence due to widespread and secure encryption. One reason for this might be that Germany has sought out lawful hacking as a way to obtain digital evidence.

It is unlikely that Germany will steer away from its current course of supporting strong, secure encryption without lawful access mechanisms. If other countries, such as the United States, mandate lawful access mechanisms, it is unclear how the German government may respond. Judging by the past developments, Germany might look for alternatives to devices with lawful access mechanisms rather than trying to force vendors and service providers to implement such mechanisms for them.

About the Authors

Sven Herpig is head of international cybersecurity policy at the Berlin-based think tank Stiftung Neue Verantwortung. Previously, Sven worked for Germany's Office for Information Security and its Foreign Office.

Stefan Heumann is co-director of Stiftung Neue Verantwortung and a member of the German parliament's expert commission on artificial intelligence.

The authors would like to thank Mirko Hohmann and an anonymous technology policy expert for their review of the manuscript.

Notes

1 On a technical level, the encryption debate in Germany is similar to debates elsewhere. It is a debate about the security level of different encryption protocols, the development of appropriate encryption standards for different technical applications, and questions regarding the most efficient and secure implementation of encryption in IT systems. Technical experts also largely agree that any form of backdoor, such as key escrow, severely undermines the security of any encryption-based security solution. But like in other countries, technical aspects are only one element of the larger debate. And this larger debate is mostly political, revolving around questions of whether and how the government can access encrypted data. Germany has a strong, long-standing commitment to not regulate encryption. We subsume this debate under the term encryption policy.

2 https://hp.kairaven.de/law/eckwertkrypto.html

3 https://www.bmwi.de/Redaktion/DE/Publikationen/Digitale-Welt/digitale-agenda.pdf?__blob=publicationFile&v=3

4 https://de.statista.com/infografik/9522/nutzung-von-ende-zu-ende-verschluesselung/

5 https://www.e-mail-made-in-germany.de/De-Mail.html

6 https://www.cr-online.de/Bundesgesetzblatt_I_54_2408.pdf

7 http://dipbt.bundestag.de/dip21/btd/18/052/1805293.pdf

8 https://www.bmi.bund.de/cybersicherheitsstrategie/BMI_CyberSicherheitsStrategie.pdf

9 https://www.stiftung-nv.de/de/publikation/transatlantic-cyber-forum-policy-debates#%E2%80%9DJanuar%E2%80%9D

10 https://www.bundesverfassungsgericht.de/pressemitteilungen/bvg08-022.html and https://www.stern.de/digital/online/online-durchsuchungen-geheimdienste-spitzeln-schon-seit-jahren-3358202.html

11 https://www.buzer.de/s1.htm?g=bkag_1997&a=20k,20l

12 https://www.stiftung-nv.de/de/publikation/transatlantic-cyber-forum-policy-debates#%E2%80%9DJune

13 https://www.bmi.bund.de/SharedDocs/downloads/DE/veroeffentlichungen/themen/ministerium/organigramm-bmi.html

[14] https://www.stiftung-nv.de/sites/default/files/snv_tcf_government_hacking-problem_analysis_0.pdf

[15] https://www.stiftung-nv.de/de/publikation/transatlantic-cyber-forum-policy-debates#%E2%80%9DJune8%E2%80%9D

[16] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/IT-Sicherheitsgesetz.pdf

[17] https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive

[18] https://www.bmjv.de/SharedDocs/Gesetzgebungsverfahren/Dokumente/NetzDG_engl.pdf?__blob=publicationFile&v=2

[19] https://ec.europa.eu/info/law/law-topic/data-protection_en

[20] https://www.stiftung-nv.de/de/publikation/transatlantic-cyber-forum-policy-debates#%E2%80%9DMaerz3%E2%80%9D

CARNEGIE
ENDOWMENT FOR
INTERNATIONAL PEACE

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

CarnegieEndowment.org