

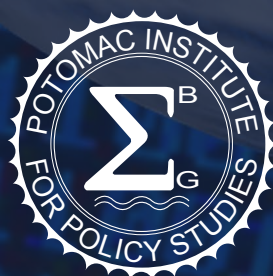


# GERMANY CYBER READINESS AT A GLANCE

Principal Investigator: Melissa Hathaway

Chris Demchak, Jason Kerben, Jennifer McArdle, Francesca Spidalieri

October 2016



Copyright © 2016, Cyber Readiness Index 2.0, All rights reserved.

Published by Potomac Institute for Policy Studies

Potomac Institute for Policy Studies  
901 N. Stuart St, Suite 1200  
Arlington, VA 22203  
[www.potomacinstitute.org](http://www.potomacinstitute.org)  
Telephone: 703.525.0770; Fax: 703.525.0299

Email: [CyberReadinessIndex2.0@potomacinstitute.org](mailto:CyberReadinessIndex2.0@potomacinstitute.org)



Follow us on Twitter:  
[@CyberReadyIndex](https://twitter.com/CyberReadyIndex)

Cover Art by Alex Taliesen.

### ***Acknowledgements***

The Potomac Institute for Policy Studies and the authors would like to thank the following individuals for their contributions: Mr. Arne Schönbohm, President of the German Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik, BSI), the BSI Executive Staff, and Dr. Sandro Gaycken, Director of the Digital Society Institute at the European School of Management and Technology (ESMT), Berlin. The authors would also like to thank Alex Taliesen for cover art and Sherry Loveless for editorial and design work.

# GERMANY CYBER READINESS AT A GLANCE

## TABLE OF CONTENTS

INTRODUCTION. . . . . 2

1. NATIONAL STRATEGY . . . . . 5

2. INCIDENT RESPONSE . . . . . 6

3. E-CRIME AND LAW ENFORCEMENT . . . . . 8

4. INFORMATION SHARING . . . . . 9

5. INVESTMENT IN RESEARCH AND DEVELOPMENT. . . . . 10

6. DIPLOMACY AND TRADE . . . . . 12

7. DEFENSE AND CRISIS RESPONSE. . . . . 14

CRI 2.0 BOTTOM LINE . . . . . 16

ENDNOTES . . . . . 17

ABOUT THE AUTHORS . . . . . 25

# GERMANY

## CYBER READINESS AT A GLANCE



Country Population	81.4 million
Population Growth	0.5%
GDP at market prices (current \$US)	\$3.356 trillion
GDP Growth	1.7%
Year Internet Introduced	1983
National Cyber Security Strategy	2011
Internet Domain	.de
Fixed broadband subscriptions per 100 users	35.8
Mobile broadband subscriptions per 100 users	63.6
Mobile phone subscriptions per 100 users	120.4

### Information and Communications Technology (ICT) Development and Connectivity Standing

International Telecommunications Union (ITU) ICT Development Index (IDI)	14	World Economic Forum's Network Readiness Index (NRI)	13
---	----	---	----

Sources: World Bank (2015), ITU (2015), NRI (2015), and Internet Society.



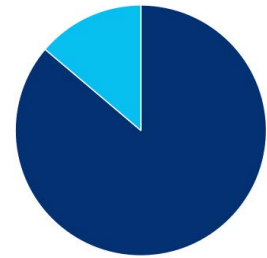
## INTRODUCTION

The Internet was first introduced in Germany in 1983 using the Bildschirmtext (BXT) – an early data network service offered by Deutsche Telekom, a government owned and operated corporation. The first email, with the banner “Willkommen CSNET,” arrived in Germany from the United States of America (US) a year later, officially establishing the German Internet.<sup>1</sup> Deutsche Telekom was the unique Internet service provider (ISP) in Germany until 1995, when German Internet access opened up to the wider commercial market. After the privatization of Deutsche Telekom, German state and federal governments continued to control about a third of its shares,<sup>2</sup> and the company is still the dominant ISP in the country.

Today, Germany is one of the world’s most technologically advanced telecommunications systems – as a result of intensive capital expenditures since its 1990 reunification – and has an Internet penetration rate of over 86 percent. The German government has been aggressively driving ICT development and Internet connectivity since the advent of the Internet and has been a pioneer in many Internet-related projects. In fact, Germany was the first country in the world to digitize its libraries after the introduction of the World Wide Web. The German Digital Libraries Project “Global Info” was launched in 1998 as part of the Information as Raw Material for Innovation program. The goal of the project was to further cooperation with universities, publishing houses, book dealers, special subject information centers, and learned societies, as well as academic and research libraries.<sup>3</sup>

Germany was also the first country in Europe to allocate spectrum in the 700 MHz band for mobile broadband by 2018. While currently only 20 percent of Germany’s rural areas have access to wireless broadband, the country’s “Digital Agenda 2014-2017” aims to remedy this problem by rolling out high-speed broadband in those more remote areas and providing all households downloads speeds of at least 50 megabits per second by 2018.<sup>4</sup> Additionally, IPv6 usage is growing significantly with over a 10 percent adoption rate, compared to an average of only 3.5 percent in the rest of the developed countries (as of April 2014).

Germany’s digital strategy has the clear scope of boosting the competitiveness, economic growth, and social well-being of the country. It highlights that enhancing high-speed networks and trust will increase “exploitation of the potential of innovation in order to achieve further growth and employment.”<sup>5</sup> The strategy envisions Germany as a leader in the Internet economy, using increased digitization and automation in manufacturing as well as promoting investment in industrial ICT applications, information technology (IT) security research, microelectronics, and other digital services. The size of the German ICT market – currently the largest in Europe and the fourth largest in the world – facilitates the German government’s ambitious plan.<sup>6</sup>



Germany Internet Penetration: 86.2%

Nonetheless, the 2016 German Defense White Paper acknowledges the major challenge of being a medium-size country, both geographically and demographically, in a rapidly changing world. Although Germany is currently the world's fourth largest economy, it realizes the unlikelihood that "in the long run ... it will retain its position."<sup>7</sup> The document recognizes the direct link between national security and economic well-being for the knowledge society of the 21st century. It also states that, "knowledge is a strategic resource for Germany" because of its particular dependence "on secure supply routes, stable markets, and functioning information and communication systems," and that "this dependence will continue to increase."<sup>8</sup>

Since 2011, the German government has also been championing what it calls the fourth industrial revolution – under the banner "Industrie 4.0" – as part of its High-Tech Strategy 2020 Action Plan.<sup>9</sup> This initiative encourages companies to adapt to the Internet of Things, especially the 3.6 million small- to medium-sized manufacturers that provide more than 60 percent of all jobs in Germany and account for about two-thirds of Germany's nearly \$4 trillion economy.<sup>10</sup> The government is investing €200 million (\$222 million) to spur Industrie 4.0 research across government, academia, and business to reap the benefits of increased connectivity in terms of improved quality, lower costs, higher efficiency, and economic growth. Chancellor Angela Merkel is urging all of Europe to embrace this initiative, too. During her address at the 2015 World Economic Forum in Davos, she stated: "those who are the leaders in the digital domain will

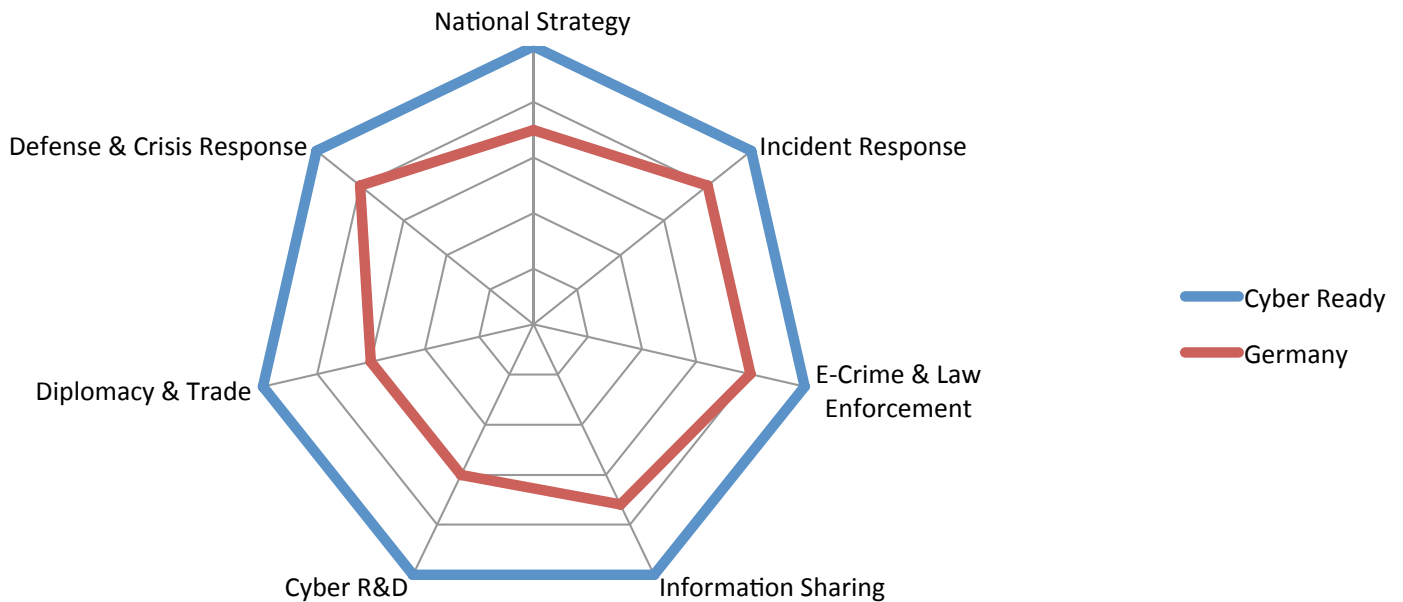
take the lead in industrial production ... it's a race we have not yet won."<sup>11</sup>

As a world leader in ICT development and adoption, Germany faces high levels of cyber crime, industrial espionage, disruption of critical services, and other malicious cyber activities. In 2012, an industry association estimated that Germany lost at least 1.5 percent of its GDP to intellectual property theft. In 2013, it was estimated that two in five German Internet users were victims of cyber crime and that an alarming number of companies and government agencies suffered cyber attacks.<sup>12</sup> In response to the growth in scope, volume, and sophistication of cyber threats, German government leaders have stated their intent to protect the value of Germany's digital investments and to preserve its national and economic security, specifically related to privacy and data protection.<sup>13</sup> However, Industrie 4.0 currently has limited investments directed toward cyber security and the innovative technologies needed to prepare for the emerging IT threats.<sup>14</sup>

Germany is leading the European dialogue regarding the need for data protection while simultaneously enabling the free flow of goods, services, people, capital, and data across borders. These objectives are a cornerstone of the European Digital Single Market initiative and are key to Europe and Germany's economic health and well-being. Germany will host the 2017 G-20 Summit in Hamburg and will likely use this event to underscore the need for all countries to develop cyber security capacity and resilience.

The Cyber Readiness Index (CRI) 2.0 has been employed to evaluate Germany's preparedness levels for cyber risks. This analysis provides an actionable blueprint for Germany to better understand its Internet-infrastructure dependencies and vulnerabilities and to assess the country's commitment and maturity in closing the gap between its current cyber security posture and the national cyber capabilities needed

to support its digital future. A full assessment of the country's cyber security-related efforts and capabilities based on the seven essential elements of the CRI 2.0 (national strategy, incident response, e-crime and law enforcement, information sharing, investment in R&D, diplomacy and trade, and defense and crisis response) follows:



German Cyber Readiness Assessment (2016)

# 1. NATIONAL STRATEGY

In 2008, the German government responded to the increasing number of infected Internet connected devices and cyber crime cases in the country by providing German citizens with a CD to help them clean up the infections on their personal devices and computers, noting that it was their national responsibility to help protect the country. By 2011, the German government adopted a more systemic and centrally supported approach with the public release of its first “Cyber Security Strategy for Germany.”<sup>15</sup> The document acknowledged the interconnections between ICTs and economic and social growth, and labeled the Internet – and its underlying ICTs – a critical infrastructure for German society.<sup>16</sup>

The national cyber security strategy highlighted several key strategic areas and objectives to better combat Germany’s cyber threat environment, including: the protection of critical infrastructure and IT systems; the strengthening of public administration’s IT security through the adoption of a uniform “federal network”; the creation of a National Cyber Response Center for incident response and protection; the establishment of a National Cyber Security Council for improved cooperation between the public sector and private sector entities; the promotion of effective international coordination for cyber security; the development of reliable and trustworthy IT through innovation; the training of skilled personnel in federal authorities; and the effective use of public sector tools – such as statutory powers – to combat cyber attacks.

*In 2011, the German government released the first “Cyber Security Strategy for Germany,” which acknowledges the interconnections between ICT and economic and social growth.*

Moreover, the document designated the Ministry of Interior’s Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik, BSI) as the national cyber security authority, responsible also for the strategy’s implementation.<sup>17</sup> The BSI was originally established in 1991 to provide IT security services for the federal government, IT manufacturers, private and commercial users, and providers of IT in Germany. As the strategy required, the BSI stood up the National Cyber Response Centre (Nationales Cyber-Abwehrzentrum, NCAZ), responsible for detecting, analyzing, and developing the necessary measures to disable potential threats.<sup>18</sup>

In accordance with the 2011 national cyber security strategy, the National Cyber Security Council was also established to enable all agencies’ State Secretaries to jointly address cyber security issues across all policies. The



Council aims to coordinate preventive tools and interdisciplinary cyber security approaches for the public and private sectors. In addition to the Federal Chancellery and representatives of the federal Länder, a State Secretary from each of the federal ministries (including the Ministry of Defense, Ministry of Interior, Ministry of Economics and Technologies, and so forth), participates in council meetings. Business representatives are also regularly invited to participate as associate members. To assist with this broad policy approach and execution, the Alliance for Cyber Security – a non-profit institution – was established by BSI in cooperation with the Federal Association for Information Technology, Telecommunications and New Media (BITKOM) in 2012. Its primary mission is to increase cyber security in Germany and to strengthen the country's resilience to cyber attacks. Toward this end, the Alliance is developing a comprehensive knowledge base and supporting an exchange of information and experiences.<sup>19</sup> Since its establishment in 2012, the Alliance has grown significantly both in membership and in engagement with cooperating partners.

Germany's 2014 digital strategy ("Digital Agenda 2014-2017") echoes elements of the national cyber security strategy by recognizing the importance of ICT for economic growth while acknowledging the need for increased security in cyberspace. The digital strategy also notes that half of German Internet users do not trust the security of their data online. Since ICT trust is essential for digital communication, e-commerce, and the achievement of a European Digital Single Market, the government is concerned about this statistic and has

taken various steps to improve trust by increasing Internet security for its citizens.<sup>20</sup> For example, BSI is currently working on implementing the 2015 IT Security Act – a core element of the national digital strategy and of its efforts to protect critical infrastructure of national importance.<sup>21</sup> These efforts include continuous cooperation with operators of critical infrastructure to identify minimum cyber security standards for critical infrastructure companies and critical infrastructure subsectors, and improving the availability, authenticity, confidentiality, and integrity of IT security throughout Germany.

In order to increase ICT security and resilience, both the cyber security strategy and the digital agenda seek also a comprehensive and multi-stakeholder approach to strengthen the security of online services and critical infrastructures. Nonetheless, more needs to be done by the German government to improve the co-ordination and interoperability between key public and private stakeholders and their IT systems, and to better prepare for emerging IT security risks related to increasing digitization of critical services across the nation's economy.

## 2. INCIDENT RESPONSE

As the national cyber security authority for Germany, BSI shapes information security policies and activities through whole-of-government and whole-of-society prevention, detection, and response, and is also the central cyber incident reporting office. The BSI issues warnings on malware and security vulnerabilities in IT products and services, distributes information to both concerned parties and the

*The German Federal Office for Information Security (BSI) is the national cyber security authority for Germany and the central cyber incident reporting office.*

general public, and recommends countermeasures.<sup>22</sup> It is also responsible for creating an information exchange with over 50,000 private institutions. Although not yet completed, the BSI's early warning alert system is modeled after the stop-light warning system used by the US Financial Services Information Sharing and Analysis Center (FS-ISAC).<sup>23</sup>

Multiple Computer Emergency Response Teams (CERTs) and equivalents have been established in Germany since 1991. In 1994, BSI established the first Computer Emergency Response Team (BSI-CERT) for federal agencies as a virtual team mainly focused on information gathering. In 2001, an official governmental CERT emerged from BSI-CERT and was renamed CERT-Bund. Since then, CERT-Bund has morphed into a formal national CERT, which serves as a platform and the central point of contact for preventive, reactive, and proactive measures regarding cyber security incidents. Today, CERT-Bund works closely with both state-level and non-governmental CERTs to offer wider range of services.

It engages proactively by monitoring, on a voluntary basis, their constituencies – including IT manufacturers and providers, and private and commercial users – for cyber security incidents. It also provides warnings, information services, active alerting, and an online reporting structure to log cyber security incidents.<sup>24</sup> In 2006, the BSI also established a Citizen's CERT (Bürger-CERT) specifically to raise cyber security awareness among the general public and small enterprises.<sup>25</sup>

While Germany does not have a consolidated, single national incident response plan, both the 2005 "National Plan for Information Infrastructure Protection," directed at both government and industry, and the 2007 "Critical Infrastructure Protection (CIP) Implementation Plan" address IT crisis response and provide recommendations for business continuity management of critical business processes in the event of a major cyber incident.<sup>26</sup> According to the 2007 CIP Plan, critical infrastructure operators had already "laid down suitable warning and alert procedures which define the units and individuals to be warned or alerted as a function of the incident discovered and the differentiation criteria for warnings and alerts."<sup>27</sup> Additionally, this Plan called for the creation of working groups for different aspects of cyber security, such as crisis management, exercises, and availability of critical services. It also outlined the agreements between the government and private operators of critical information infrastructure on how to fulfill the necessary tasks of protecting those infrastructures and to respond effectively and in a concerted manner to IT security incidents.

The 2011 national cyber security strategy instructed the BSI to establish the National Cyber Response Centre (Nationales Cyber-Abwehrzentrum, NCAZ), responsible for better coordination of incident response and more timely information sharing between government and the private sector. In the role of a national command, control, and analysis center, the BSI's NCAZ was intended to enable "all competent bodies to respond rapidly to serious incidents, and [to] provide incident analyses and assessments to all relevant bodies and coordinates the cooperation with local and sector-internal crisis management organizations."<sup>28</sup> In addition to the direct involvement of the Federal Office for the Protection of the Constitution (Bundesamt für Verfassungsschutz, BfV) and the Federal Office of Civil Protection and Disaster Assistance (Bundesamt für Bevölkerungsschutz und Katastrophenhilfe, BBK), all other government authorities dealing with cyber security issues – including the Federal Criminal Police Office (Bundeskriminalamt, BKA), the Federal Police (Bundespolizei, BPOL), the Customs Criminological Office (Zollkriminalamt, ZKA), the Federal Intelligence Service (Bundesnachrichtendienst, BND), the Bundeswehr, and other authorities supervising critical infrastructure operators – participate in the center and work closely and directly with each other and with the private sector. The German digital agenda promises future strengthening of the center's incident response capacities.

Germany has conducted several national cyber security exercises to practice crisis response plans for government agencies and specific

operators of critical infrastructure. One of these, a 2011 crisis planning and readiness exercise, aimed to understand government response procedures for a multi-pronged attack including distributed denial of service attacks against critical infrastructures, the injection of malware into the banking system, and the insertion of false traffic within air traffic control systems.<sup>29</sup> Germany also participates in multi-national exercises organized by the European Union and the North Atlantic Treaty Organization (NATO). Despite the number of exercises conducted in recent years, the CIP implementation plan recommended that more "exercises should be carried out in order to validate and update existing concepts."

Finally, the BfV – Germany's domestic intelligence agency – publishes annual cyber threat reports. The 2016 report stated that Russia and China are the leading sources of cyber attacks on Germany. It also revealed that Germany has detected Iranian information security threats against a number of victims.<sup>30</sup>

### **3. E-CRIME AND LAW ENFORCEMENT**

Germany has demonstrated international commitment to protect society against cyber crime by signing (2001) and ratifying (2009) the Council of Europe Convention on Cybercrime – commonly known as the Budapest Convention – as well as by working domestically to enforce it. As well, Germany has signed and ratified the Additional Protocols to the Convention on Cyber Crime, which concerns the criminalization of racist and xenophobic-natured acts committed

through computer systems. In its 2011 national cyber security strategy, Germany reaffirmed its commitment to work toward international harmonization in criminal law based on the Budapest Convention.

In July 2015, Germany established a new IT Security Act with the goal of preventing the loss of important IT systems such as those used by the BSI, telecommunications providers, critical infrastructure operators, and others. BSI is currently working to implement this Act, which includes minimum cyber security standards for over 2,000 critical infrastructure companies. In accordance with the law, these minimum security requirements are being supported by improvements of the availability, authenticity, confidentiality, and integrity of IT security throughout Germany; increased Internet security for citizens; and better protection of critical infrastructure of national importance.<sup>31</sup> In addition, Germany has other laws that directly prohibit cyber crimes such as computer fraud, data tampering, computer sabotage, data espionage, phishing, as well as other related cyber crimes through the prosecution of the traditional crime statutes.<sup>32</sup> Within two years of adoption of the regulation, all covered operators are supposed to implement appropriate organizational and technical security measures to protect the IT systems, components, or processes relevant for the functioning of the critical infrastructures. These security measures must accommodate state-of-the-art technology. Further, operators of critical infrastructures are obliged to undergo IT security audits or certifications at least every two years, and they may suggest industry-specific security standards.

In terms of law enforcement, Germany has established a mature institutional ability to address different elements of cyber crime. The National Cyber Response Center, BSI, and the Federal Criminal Police Agency (BKA) jointly lead the national cyber crime efforts. In particular, the National Cyber Response Center combines resources from various government agencies, including the federal police and foreign intelligence agency, and from industry.<sup>33</sup>

The 2011 national cyber security strategy promised to strengthen the capabilities of law enforcement agencies, the BSI, and the private sector in combating cyber crime, as well as to protect the country against espionage and sabotage. Germany has “set up joint institutions with industry with the participation of the competent law enforcement agencies.”<sup>34</sup> As shown by the 2015 IT Security ACT, there is further progress to be made to successfully implement these ambitions. The end of 2017 will indicate to what extent government and industry have successfully worked together to further the country’s ability to significantly reduce cyber crime. With this in mind, it is unclear whether there are sufficient initiatives to train court judges, prosecutors, lawyers, law enforcement officials, forensic specialists, and other investigators.

## 4. INFORMATION SHARING

As stated in the 2011 national cyber security strategy, the German National Cyber Response Centre is responsible for both incident response coordination and whole-of-society information sharing. Information shared includes weak-

*The German National Cyber Response Centre is responsible for both incident response coordination and whole-of-society information sharing.*

nesses of IT products, vulnerabilities, forms of attacks, profiles or perpetrators, and so forth. One critical need is to have an organization composed of industry and other non-governmental actors able to provide current and valid information in the area of cyber security nationwide, and to advise stakeholders in preparing and mitigating cyber incidents. In collaboration with the National Cyber Response Center, the Alliance for Cyber Security – a platform for cooperation and information exchange created in 2012 – meets this need. It facilitates close collaboration among partners in the economic, academic, and administrative fields, and with enterprises of special public interest.

Contributing to national information sharing, the National Information Technology Situation Centre (Nationales IT-Lagezentrum), operated by the BSI, keeps track of the national and global IT security situation, in order to rapidly detect and analyze major IT security incidents and recommend protective measures. In case of an IT-related crisis, it can expand its capacity and be transformed into the National Information

Technology Crisis Reaction Centre (Nationales IT-Krisenreaktionszentrum). This center concentrates capabilities for handling IT crises, covering all national aspects, including governmental networks and critical infrastructures.

Moreover, Germany participates in various intra-state and inter-agency partnerships to foster information sharing. For instance, the US-Germany Cyber Bilateral Meeting serves as a recognized partnership to facilitate sharing of cyber security assets across borders.<sup>35</sup> Germany is also part of the National Cyber Forensics and Training Alliance (NCFTA), a US non-profit corporation with a mission to facilitate collaboration among private industry, academia, and law enforcement to identify, mitigate, and neutralize complex cyber-related threats.<sup>36</sup>

Implementation of many information sharing initiatives may face challenges because Germany has both federal and state policies and programs. The ability to respond to the most advanced and sophisticated threat methods vary from state to state because each state has different cyber security capabilities and maturity levels. Information sharing is critical for implementation of all central government's efforts, but may be difficult to achieve in the near term.

## **5. INVESTMENT IN RESEARCH AND DEVELOPMENT**

The 2011 national cyber security strategy advocated for an intensification of research on IT security and critical infrastructure as a core



strategic area for future implementation. The Germany's 2014 national digital agenda highlighted the need for extensive investments in industrial ICT applications, IT security research, microelectronics, and digital services – in short, an all-of-the-nation cyber research and development (R&D) effort.<sup>37</sup> In accordance with the digital agenda, Germany has established two big data centers in Berlin in order to promote big data driven innovation and industrial applications, science, and healthcare.<sup>38</sup>

In March 2015, the German government released a plan to promote IT security R&D, entitled "Self-Determination and Safety in the Digital World 2015-2020." The plan included a budget of €180 million (~\$198 million) through 2020 intended to promote specific encryption technologies and further protection of personal data and communications services. The plan focused on four key areas: new technologies; secure and trustworthy information and communication systems; application areas of IT security; and privacy and protection of data.

In order to help drive the government's R&D mission, the German Ministry of Education and Research (BMBF) established three centers for IT security in three different universities: the Center for IT Security, Privacy and Accountability (CISPA) in Saarbrücken; the European Center for Security and Privacy by Design (EC-SPRIDE) in Darmstadt; and the Competence Center for Applied Security Technology (KASTEL) in Karlsruhe. In 2009, BMBF and the Ministry of the Interior agreed also to a joint cooperation project in IT R&D, thus establishing the "IT Security Research" working program to research and discover new IT security applications.<sup>39</sup>

*The government has recognized that in order to ensure the sustainability of Germany IT security research, more qualified personnel must be trained.*

Furthermore, the government has recognized that in order to ensure the sustainability of Germany IT security research, more qualified personnel must be trained. Students at the BMBF-funded KASTEL competence center are encouraged to gain a certificate as specialist in the field of IT security, which is comparable to a specialized master's degree. The Technische Universität Darmstadt has been offering a Master of Science (M.S.) degree course in IT Security since 2010. Employed professionals are also able to attend courses on security fundamentals at the Center for Advanced Security Research Darmstadt (CASED) at Technische Universität Darmstadt, leading to a certificate in IT security. The University of Freiburg Department of Computer Science offers a M.S. in Computer Science, which allows students to specialize in cyber security. Moreover, the program allows students to take additional courses in political science and other social science disciplines, which give a more holistic understanding of cyber security issues.<sup>40</sup>

In addition, the German government now provides corporate R&D incentives related to

cyber security in three major areas: “computer technology – working in a digitized world”; “ICT –detecting and solving cybersecurity incidents”; and “e-mobility – value chain proposition.” The first two areas are open to all industry sectors, whereas the final area is open only to the production and ICT sectors. Incentives include non-repayable cash grants to companies, consortium, and research institutions.<sup>41</sup> Most recently, the government has also underscored the importance of venture capital investments (VC) in the ICT sector, with a particular focus on support for IT start-ups. In order to help spur IT start-up growth, the government provides also some VC assistance, to include: information and advice for founders; improvements to financing through competitive work conditions and crowd investments; linking start-ups to traditional businesses with related market activities; and through the creation of international start-up “hubs,” including business incubators.<sup>42</sup>

As Germany prepares to hold the G-20 presidency and host the G-20 Summit in Hamburg in 2017, the country as a whole will also have an opportunity to demonstrate its leadership in ICT innovation and research. Indeed, in June 2016, the University of Hamburg received €1 million (\$1.10 million) in EU funding for a cyber security research project at the University. The University of Hamburg and Schleswig-Holstein’s Independent Center for Privacy Protection have joined nine other institutions in seven countries to form the “Constructive an Alliance for Value-driven Cybersecurity (CANVAS) research network.” Researchers in CANVAS will investigate how to balance cyber security and basic democratic values in

three main application areas: healthcare sector, financial systems, and national security.<sup>43</sup>

Nonetheless, Germany faces a significant shortage of cyber security professionals, especially in government service. The Federal Ministry of Education and Research is funding the establishment of a new institute – the German Internet Institute (Deutsches Internet Institut, DII) – and will invest as much as €50 million (~\$56 million) for its development over the next five years. The Institute will explore the ethical, legal, economic, and participatory aspects of Internet and digitization in an interdisciplinary approach.<sup>44</sup> In addition, the Einstein Foundation and the state of Berlin are creating the Einstein Center of Digital Future (ECDF) – a new public-private partnership for research on the digitization of German society – and are investing €38.5 million (~\$43million) in fifty new professorships on digital, including IT security.<sup>45</sup> The new Einstein Center will connect several public entities and universities, including Technische Universität Berlin, Freie Universität Berlin, Humboldt-Universität zu Berlin, Universität der Künste Berlin and Charité – Universitätsmedizin Berlin, with eight renowned research institutes and two other universities of applied sciences.

## **6. DIPLOMACY AND TRADE**

Germany has been actively engaged in diplomatic and trade and commerce negotiations related to cyber security for some years. It is also the lead negotiator for the Privacy Shield and other data protection initiatives within the EU, as well as those between the EU and the US.

In the 2011 national cyber security strategy, Germany recognized that, “given the global nature of information and communications technology, international coordination ... focusing on foreign and security policy aspects, ...[is] indispensable.”<sup>46</sup> Indeed, Germany has been very active in the international arena, including collaboration with the United Nations (UN), the EU, the Council of Europe, the North Atlantic Treaty Organization (NATO), the G-7, the Organization for Security and Cooperation in Europe (OSCE), and other multinational organizations. The multi-stakeholder theme expressed in the national cyber security strategy was reiterated in its Digital Agenda 2014-2017, and is actively pursued in the following fora: International Telecommunication Union (ITU), Internet Governance Forum (IGF), Organization for Economic Co-operation and Development (OECD), and the UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications (GGE). In particular, Germany has shown its commitment to influence the international discussion on cyber-related matters by its consistent participation in all Cyber-GGEs.

In addition, Germany engages in dialogues on cyber issues with a variety of partners, both formally and informally, and participates in conferences and discussions around the world. Germany’s digital agenda reinforced the connections between economics and cyber security. For instance, Germany routinely addresses development cooperation issues and participates in projects dedicated to cyber capacity building, cyber security capacity building, and cyber confidence building in developing countries.

On March 2016, the US and Germany promised to collaborate on the protection of critical infrastructure, and to “continue to work closely to enhance cybersecurity of critical infrastructure, improve incident management and coordination, and build cyber capacity of other countries.”<sup>47</sup> As part of this Transatlantic Cyber Dialogue, the US and Germany are also discussing the recent proposal for an intra-Germany routing system, encryption issues, and a new standard process for hardware and software.

In 2011, the Ministry of Foreign Affairs established an International Cyber Policy Coordination Staff in the Federal Foreign Office intended to work with other ministries and actors to develop a foreign policy promoting a free, open, secure, and stable cyberspace. The Federal Foreign Office sees international cyber policy as a crosscutting task impacting on virtually all areas of foreign policy. Among its objectives, this policy seeks to facilitate the economic opportunities the Internet offers, the responsible use of the Internet, and the

*The Ministry of Foreign Affairs has established an International Cyber Policy Coordination Staff and the role of Ambassador for Cyber.*

security of cyberspace.<sup>48</sup> Main international priorities for the work of the Federal Foreign Office in these fora are, among others, agreement on standards for good governance, the application of international law, as well as the development of confidence-building measures for more cyber security. Germany has also established the role of Ambassador for Cyber in a number of major cities, who respond to this dedicated section of the German Ministry of Foreign Affairs.

## 7. DEFENSE AND CRISIS RESPONSE

In July 2016, the German Ministry of Defense (MOD) released their new “White Paper on German Security Policy and the Future of the Bundeswehr,” which highlights cyber risks as a top-tier national threat.<sup>49</sup> The Defense White Paper recognizes that “the cyber and information domain has become an area of international and strategic importance that has practically no limits, [and that] its significance will continue to grow.”<sup>50</sup> The government’s new policy sees Germany as a “key player” in Europe and outlines Germany’s “responsibility to actively help shape the global order.”

In this document, the “defence aspects of whole-of-government cyber security are [listed as] core tasks of the Federal Ministry of Defence and the Bundeswehr” (i.e., the German uniformed services). Furthermore, the MOD is responsible for developing national capabilities, which “promote a whole-of-government approach and cooperate with re-

search institutions, industry and partners.”<sup>51</sup> A key component of this plan is for Germany to have a strong cyber defense posture and military that is capable of “defending Germany’s freedom in cyber space.”

In April 2016, Germany began the process of standing up a cyber and information command within a relatively short period after Defense Minister Ursula von der Leyen announced this intention in September 2015.<sup>52</sup> The new organization, Cyber and Information Space Command (Kommando Cyber und Informationsraum, KCIR), merges the Bundeswehr’s existing cyber-related units and is responsible for cyber, IT (networks), military intelligence, geo-information, and operative communication.<sup>53</sup> It is expected to be fully operational by 1 April 2017, and will be led by a lieutenant general. The KCIR plans to have 13,500 personnel that will primarily come from individuals already in other military services and organizations, distributed

*In 2016, Germany began the process of standing up a Cyber and Information Space Command.*

across the Command and two new centers – a cyber operations centre and a Bundeswehr cyber security centre.<sup>54</sup> Finding sufficient numbers of IT-skilled talent is as difficult for the Bundeswehr as it is for any other public agency. Nonetheless, the Bundeswehr is hoping to attract another 800 experts by the end of the current year, using the recruiting slogan “Defending Germany’s Freedom in Cyberspace.”<sup>55</sup>

The German MOD has also stated that it wants the Bundeswehr to have the ability to strike back with its own cyber force and envisions this new Cyber Command to enable Germany to cooperate on the same level with other nations, such as the US. The Department of Information and Computer Network Operations, within the Bundeswehr’s Strategic Reconnaissance Unit, is focused on developing largely defensive capabilities. After extensive legal analysis in the early 2000s, the MOD began limited efforts in 2005 to develop some potentially offensive capabilities – such as red teaming – with the understanding that the skills of this top secret cyber warfare unit would be used only for defensive purposes.<sup>56</sup> The MOD is also looking to top schools in the country, like the European School of Management and Technology (ESMT), to support its requirements for advanced research and specialized training.

The German government prefers to keep its defensive cyber security efforts separate from its intelligence services. In 2011, the

German government set up a National Cyber Response Centre under the Ministry of the Interior. The Center combines resources from various government agencies, including the federal police and foreign intelligence agency, and even industry, and reports to the Federal Office for Information Security.<sup>57</sup> This facility was initially staffed with few employees from BSI, the German Office for the Protection of the Constitution, and the BBK. Since its establishment, the Federal Police, Federal Office of Criminal Investigation, the German National Intelligence Service (BND), the Bundeswehr, and the Customs Criminal Investigation Office (ZKA) have all placed experts in the response centre. The National Cyber Security Council is also responsible for coordinating defense techniques and cyber policy. Senior military representatives are among the staff.<sup>58</sup>

While the MOD’s capabilities in cyberspace and in the cyber defense of the nation have been expanded and elevated in significance, the government is proposing to tighten controls over the BND and to impose new legal restrictions on its surveillance activities. These legal reforms, which must still be finalized by the German parliament, would ban the BND from spying on countries, citizens, and institutions in the EU, except in the case of suspected terrorist activity.<sup>59</sup> The agreement would also require the head of the BND, the Chancellor’s office, and an independent panel of judges to approve strategic foreign espionage activities based on keyword lists. This differs from many other countries that directly



link their intelligence services with their military cyber capabilities.

## CRI 2.0 BOTTOM LINE




According to the CRI 2.0 assessment, Germany is on a path to becoming cyber ready and is currently partially operational in all of the seven CRI essential elements.

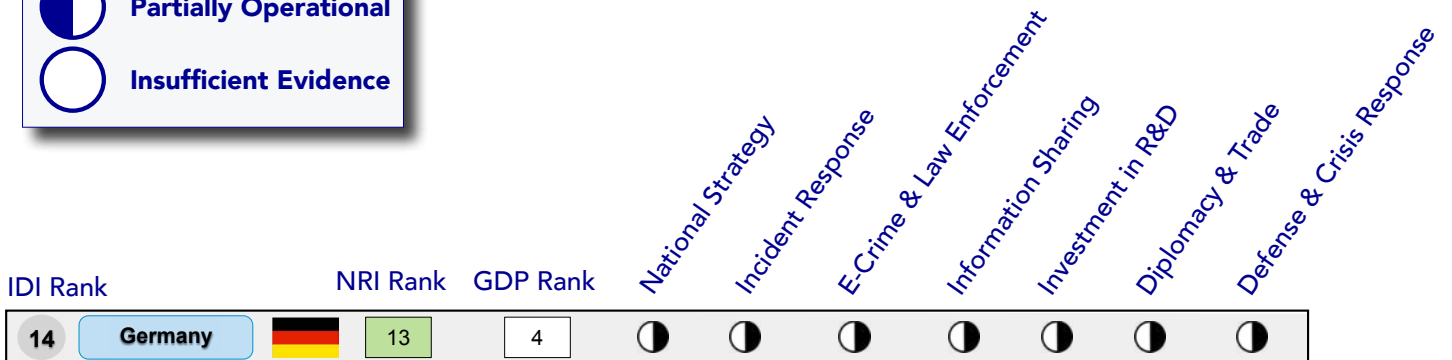
The findings in this analysis represent a snapshot in time of a dynamic and changing landscape. As Germany continues to develop and update its economic (digital agenda) and na-

tional cyber security strategies, policies, and initiatives to reflect a more balanced approach that aligns its national economic visions with its national security priorities, updates to this country profile will reflect those changes and monitor, track, and evaluate substantive and notable improvements.

The CRI 2.0 offers a comprehensive, comparative, experience-based methodology to help national leaders chart a path towards a safer, more resilient digital future in a deeply cybered, competitive, and conflict prone world. For more information regarding the CRI 2.0, please see: <http://www.potomac institute.org/academic-centers/cyber-readiness-index>.

**Legend**

-  Fully Operational
-  Partially Operational
-  Insufficient Evidence



## ENDNOTES

1. Internet Hall of Fame, "Timeline," <http://www.internethalloffame.org/internet-history/timeline>.
2. Deutsche Telekom, "Shareholder Structure," <https://www.telekom.com/shareholder-structure>.
3. Diann Rusch-Feja and Hans Jurgen Becker, "Global Info: the German Digital Libraries Project," *D-Lib Magazine*, vol.5 no. 4 (April 1999), <http://www.dlib.org/dlib/april99/04rusch-feja.html>.
4. The Federal Government, "Digital Agenda 2014-2017," (2014): 21, [https://www.digitale-agenda.de/Content/DE/\\_Anlagen/2014/08/2014-08-20-digitale-agenda-engl.pdf?\\_\\_blob=publicationFile&v=6](https://www.digitale-agenda.de/Content/DE/_Anlagen/2014/08/2014-08-20-digitale-agenda-engl.pdf?__blob=publicationFile&v=6).
5. *Ibid.*
6. Federal Ministry of Economic Affairs and Federal Ministry of Labour and Social Affairs, "IT and Telecommunication," (2014), <http://www.make-it-in-germany.com/en/for-qualified-professionals/working/industry-profiles/it-and-telecommunications>.
7. The Federal Government, "2016 White Paper on German Security Policy and the Future of the Bundeswehr," (July 2016): 22, <https://www.bmvg.de/portal/a/bmvg/en/>.
8. *Ibid.*
9. Matthew Karnitschnig, "Why Europe's Largest Economy Resists New Industrial Revolution," *Politico*, July 6, 2016, <http://www.politico.eu/article/why-europes-largest-economy-resists-new-industrial-revolution-factories-of-the-future-special-report/>.
10. Federal Ministry for Economic Affairs and Energy, "Introducing the German Mittelstand," <http://www.make-it-in-germany.com/en/for-qualified-professionals/working/mittelstand>.
11. Sara Zaske, "Germany's Vision for Industrie 4.0: The Revolution will be Digitized," *ZDNet*, February 23, 2015, <http://www.zdnet.com/article/germanys-vision-for-industrie-4-0-the-revolution-will-be-digitised/>.
12. "Two in Five Internet Users in Germany Hit by Cybercrime in 2013," *eMarketer*, May 21, 2014, <http://www.emarketer.com/Article/Two-Five-Internet-Users-Germany-Hit-by-Cybercrime-2013/1010845>.
13. "Merkel: 'Difficulties Yet to Overcome' in US Spy Scandal," *CBS DC*, May 2, 2014, <http://washington.cbslocal.com/2014/05/02/merkel-difficulties-yet-to-overcome-in-us-spy-scandal/>.
14. Melissa Hathaway's interview with Dr. Sandro Gaycken, Director of the Digital Society Institute, ESMT Berlin, September 20, 2016.

15. Federal Ministry of the Interior, "Cyber Security Strategy for Germany," (2011), [https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/CyberSecurity/Cyber\\_Security\\_Strategy\\_for\\_Germany.pdf?\\_\\_blob=publicationFile](https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/CyberSecurity/Cyber_Security_Strategy_for_Germany.pdf?__blob=publicationFile).
16. Flippa von Stackelberg, "Germany Prepares for Cyber War," *New Security Learning*, <http://www.newsecuritylearning.com/index.php/feature/88-germany-prepares-for-a-cyber-war>.
17. Federal Ministry of the Interior, "Cyber Security Strategy for Germany."
18. The new National Cyber Response Centre pools the cyber defense resources of the Federal Office for Information Security, the Federal Office for the Protection of the Constitution, the Federal Intelligence Service, the Federal Police, the Customs Criminal Investigation Office, the German Military, the Federal Office of Civil Protection and Disaster Assistance, and the Federal Criminal Police Office; and it will cooperate with ISPs.
19. TÜViT, "Alliance for Cyber Security," <https://www.tuvit.de/en/cyber-security/alliance-for-cyber-security-2352.htm>.
20. Federal Government, "Digital Agenda 2014-2017," 5.
21. Federal Office for Information Security, "The State of IT Security in Germany 2015," (2015): 42, [https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Securitysituation/IT-Security-Situation-in-Germany-2015.pdf?\\_\\_blob=publicationFile&v=2](https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Securitysituation/IT-Security-Situation-in-Germany-2015.pdf?__blob=publicationFile&v=2).
22. Federal Office for Information Security, "Annual Report," (2003): 27, [https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/annualreport/BSI-AnnualReport2003.pdf?\\_\\_blob=publicationFile](https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/annualreport/BSI-AnnualReport2003.pdf?__blob=publicationFile).
23. Melissa Hathaway's interview with Arne Schonbohm, Director of BSI, June 8, 2016, in Berlin, Germany.
24. Federal Office of Information Security, "CERT-Bund," [https://www.bsi.bund.de/EN/Topics/IT-Crisis-Management/Cert-Bund/cert-bund\\_node.html](https://www.bsi.bund.de/EN/Topics/IT-Crisis-Management/Cert-Bund/cert-bund_node.html).
25. Bürger CERT, "About Us," <https://www.buerger-cert.de/about>.
26. Federal Ministry of the Interior, "National Plan for Information Infrastructure Protection," (2009), <http://www.qcert.org/sites/default/files/public/documents/GER-PL-National%20Plan%20For%20Information%20Infrastructure%20Protection-Eng-2005.pdf>, and "CIP Implementation Plan for Information Infrastructure Protection," (2007) <http://www.bmi.bund.de/SharedDocs/Downloads/EN/Broschueren/2009/kritis.html>.

27. Federal Ministry of the Interior, "CIP Implementation Plan for Information Infrastructure Protection."
28. Federal Ministry of the Interior, "Cyber Security Strategy for Germany."
29. Melissa Hathaway, "Best Practices in Computer Network Defense: Incident Detection and Response," NATO Science for Peace and Security Series, Information and Communications Security, vol.35, (IOS Press, February 2014): 12, <http://www.iospress.nl/book/best-practices-in-computer-network-defense-incident-detection-and-response/>.
30. Joe Uchill, "German Intelligence Blames Russia, China for Cyberattacks," *The Hill*, June 28, 2016, [http://thehill.com/policy/cybersecurity/285202-german-intelligence-blames-russia-china-for-cyber-attacks?utm\\_source=&utm\\_medium=email&utm\\_campaign=2679](http://thehill.com/policy/cybersecurity/285202-german-intelligence-blames-russia-china-for-cyber-attacks?utm_source=&utm_medium=email&utm_campaign=2679).
31. Watson Farley & Williams, "Briefing: The New German IT Security Act," February 2016, <http://www.wfw.com/wp-content/uploads/2016/02/WFW-Briefing-Germany-IT-Security-Feb-2016-EN-15-Feb.pdf>.
32. Federal Ministry of Justice and Consumer Protection, (2015), [http://www.gesetze-im-internet.de/englisch\\_stgb/index.html](http://www.gesetze-im-internet.de/englisch_stgb/index.html).
33. Center for Strategic and International Studies, "Cybersecurity and Cyberwarfare," (2011), <http://unidir.org/files/publications/pdfs/cybersecurity-and-cyberwarfare-preliminary-assessment-of-national-doctrine-and-organization-380.pdf>.
34. Federal Ministry of the Interior, "Cyber Security Strategy for Germany," 10.
35. US Department of State, "Joint Statement on US-Germany Cyber Bilateral Meeting," June 27, 2014, <http://www.state.gov/r/pa/prs/ps/2014/06/228543.htm>.
36. National Cyber-Forensics & Training Alliance, "Become a NCFTA Partner," <https://www.ncfta.net>.
37. Federal Government, "Digital Agenda 2014-2017."
38. Federal Ministry of Education and Research, "Berlin Big Data Center," <http://www.bbdc.berlin/start/>.
39. Federal Ministry of the Interior, "Cyber Security Strategy for Germany," (2011): 11, and Federal Ministry of Education and Research, "Digital World: Cybersecurity Research to Boost Germany's Competitiveness," <https://www.bmbf.de/en/cybersecurity-research-to-boost-germany-s-competitiveness-1418.html>.
40. University of Freiburg, "Department of Computer Science," <http://www.informatik.uni-freiburg.de/studies/studies>.

41. Deloitte, "Grants and Incentive Program Updates: The Latest Legislative Developments From Around the World," (April 2015), <https://www2.deloitte.com/content/dam/Deloitte/nl/Documents/tax/deloitte-nl-tax-grants-and-incentives-newsletter-april-2015.pdf>, and Deloitte, "2014 Global Survey of R&D Tax Incentives," (March 2014): 17, <http://www2.deloitte.com/content/dam/Deloitte/global/Documents/Tax/dttl-tax-global-rd-survey-aug-2014.pdf>.
42. OECD, "OECD Digital Economy Outlook 2015," (July 15, 2015): 25, <http://www.oecd.org/internet/oecd-digital-economy-outlook-2015-9789264232440-en.htm>.
43. "1 Million Euro for Cyber Security Project at Hamburg University," *Hamburg News*, June 21, 2016, <http://www.hamburg-news.hamburg/en/cluster/media-it/eu-funds-research-project-ethical-cyberspace/>.
44. Georg Schütte, State Secretary at the Federal Ministry of Education and Research, "New Year's Reception for the Science Counsellors of the Foreign Embassies," January 25, 2016, <https://www.bmbf.de/de/the-ccasion-of-the-new-year-s-reception-for-the-science-counsellors-of-the-foreign-2381.html>.
45. Melissa Hathaway's interview with Professor Philip Lark, September 26, 2016. For more information on the Einstein Center of Digital Future (ECDF), see: <http://be-digital.berlin/the-einstein-center-digital-future/>.
46. Federal Ministry of the Interior, "Cyber Security Strategy for Germany."
47. US Department of State, "Joint Statement on US-Germany Cyber Bilateral Meeting," March 24, 2016, <http://www.state.gov/r/pa/prs/ps/2016/03/255082.htm>.
48. Federal Foreign Office, "International Cyber Policy," [http://www.auswaertiges-amt.de/EN/Aussenpolitik/GlobaleFragen/Cyber-Aussenpolitik/KS-Cyber-Aussenpolitik\\_node.html](http://www.auswaertiges-amt.de/EN/Aussenpolitik/GlobaleFragen/Cyber-Aussenpolitik/KS-Cyber-Aussenpolitik_node.html).
49. The Federal Government, "2016 White Paper on German Security Policy and the Future of the Bundeswehr." Germany's Defense White Papers are released periodically; the previous one was released in 2011.
50. *Ibid*, 37.
51. *Ibid*, 93.
52. Federal Ministry of Defense, "Keynote Address by Minister von der Leyen at Cyber-Workshop," September 17, 2015, [https://www.bmvg.de/portal/a/bmvg/!ut/p/c4/NYy7CsJAEEX\\_aCYrg-mCXkBSCjTYaG9nsDnFgH2Gcrl-0fb7bwHjjNgYsP3Ei28GyVc7IB-7zg6Pk4fmGKZla5BOZJnC4U9ZSvux-QU80zNy4reScMJbffeELifSaqWkvHk-Wq1lgyaKhllVkk8Aex8b0XWOa\\_8y33-Q3D5WwO-\\_7UXXGJsf0B62YR2w!!/](https://www.bmvg.de/portal/a/bmvg/!ut/p/c4/NYy7CsJAEEX_aCYrg-mCXkBSCjTYaG9nsDnFgH2Gcrl-0fb7bwHjjNgYsP3Ei28GyVc7IB-7zg6Pk4fmGKZla5BOZJnC4U9ZSvux-QU80zNy4reScMJbffeELifSaqWkvHk-Wq1lgyaKhllVkk8Aex8b0XWOa_8y33-Q3D5WwO-_7UXXGJsf0B62YR2w!!/).
53. Until this move, the Bundeswehr (i.e., the German uniformed services) like



most modern militaries divided missions between cyber operations units and IT or network units. This new command merges these units in a model similar to that of the US Navy's Fleet Cyber/C10F organizational structure. The speed of this establishment and its innovative structure is a highly unusual step for the German MOD and a testament to the government's intent to both defend itself and to have greater influence on international cyber matters.

54. Federal Ministry of Defense, "Final Report: Building the Cyber and Information Space Command," [https://www.bmvg.de/portal/a/bmvg/!ut/p/c4/NYyxDslwDAX\\_yE4WRNIadYENpArKl-jZRsRQnlXHCwsfTDryTbjnp4RM3kqu0OK-WcXMQHjjOdp9MXBfgEpU4eH-JQyYfsZH5RBaZEbw1ChfG-X\\_gAc05Bd-2tSpsXcZoF1iwa91JEtgLkcTS274w1\\_9lv2\\_SX4Xo4Nv25u-HK3P4AaMgbvg!!/](https://www.bmvg.de/portal/a/bmvg/!ut/p/c4/NYyxDslwDAX_yE4WRNIadYENpArKl-jZRsRQnlXHCwsfTDryTbjnp4RM3kqu0OK-WcXMQHjjOdp9MXBfgEpU4eH-JQyYfsZH5RBaZEbw1ChfG-X_gAc05Bd-2tSpsXcZoF1iwa91JEtgLkcTS274w1_9lv2_SX4Xo4Nv25u-HK3P4AaMgbvg!!/).
55. Christoph Hickmann, "Call to Arms for Cyber War, Trying to Poach Private Sector Recruits," *Süddeutsche Zeitung*, April 18, 2016, <http://international.sueddeutsche.de/post/143005903195/call-to-arms-for-cyber-war-trying-to-poach>.
56. "Germany Reveals Offensive Cyberwarfare Capability," *Atlantic Council*, June 8, 2012, <http://www.atlanticcouncil.org/blogs/natosource/germany-reveals-offensive-cyberwarfare-capability>.
57. James Lewis and Katrina Timlin, "Cybersecurity and Cyberwarfare," Center for Strategic and International Studies, (2011): 12-13, <http://unidir.org/files/publications/pdfs/cybersecurity-and-cyberwarfare-preliminary-assessment-of-national-doctrine-and-organization-380.pdf>.
58. Federal Ministry of the Interior, "Cyber Security Strategy for Germany," 8-10.
59. Thorsten Severin and Andrea Shalal, "German Government Agrees to Reform BND Spy Agency – Sources," *Reuters*, June 3, 2016, <http://af.reuters.com/article/worldNews/idAFKCN0YP2KG>.

*For more information or to provide data to the  
CRI 2.0 methodology, please contact:  
[CyberReadinessIndex2.0@potomacinstitute.org](mailto:CyberReadinessIndex2.0@potomacinstitute.org)*

## ABOUT THE AUTHORS

**Melissa Hathaway** is a leading expert in cyberspace policy and cybersecurity. She serves as a Senior Fellow and a member of the Board of Regents at Potomac Institute for Policy Studies and is a Senior Advisor at Harvard Kennedy School's Belfer Center for Science and International Affairs. She served in two Presidential administrations where she spearheaded the Cyberspace Policy Review for President Barak Obama and led the Comprehensive National Cybersecurity Initiative for President George W. Bush. She developed a unique methodology for evaluating and measuring the level of preparedness for certain cybersecurity risks, known as the Cyber Readiness Index. She publishes regularly on cybersecurity matters affecting companies and countries. Most of her articles can be found at the following website: [http://belfercenter.ksg.harvard.edu/experts/2132/melissa\\_hathaway.html](http://belfercenter.ksg.harvard.edu/experts/2132/melissa_hathaway.html).

**Chris Demchak** is a subject-matter expert on the Potomac Institute for Policy Studies' Cyber Readiness Index project. Her research areas are digital resilience, cyber conflict, and the structures and risks of cyber space. She designed a digitized organization model known as "Atrium" that helps large enterprises respond to and accommodate surprises in their systems. She is also the author of *Wars of Disruption and Resilience: Cybered Conflict, Power and National Security*.

**Jason Kerben** is a subject-matter expert on the Potomac Institute for Policy Studies' Cyber Readiness Index project. He also serves as senior advisor to multiple Departments and Agencies in matters related to information security and cyber security. In particular, he focuses on legal and regulatory regimes that impact an organization's mission. He develops methodologies and approaches to assess and manage cyber security risk and advises on a myriad of specific cybersecurity activities including international principles governing information and communications technologies, identity and access management, continuous diagnostics and mitigation and cyber insurance.

**Jennifer McArdle** is a Non-Resident Fellow at the Potomac Institute for Policy Studies and an Assistant Professor of Cybersecurity at Salve Regina University in Newport, RI. Jennifer's academic research and publications focus on cyber conflict, escalation management, and military innovation. She is a PhD candidate in War Studies at King's College London.

**Francesca Spidalieri** is a subject-matter expert at the Potomac Institute for Policy Studies' Cyber Readiness Index Project. She also serves as the Senior Fellow for Cyber Leadership at the Pell Center, at Salve Regina University, and as a Distinguished Fellow at the Ponemon Institute. Her academic research and publications focus on cyber leadership development, cyber risk management, cyber education, and cyber security workforce development. She also published a report, entitled *State of the States on Cybersecurity*, that applies the Cyber Readiness Index 1.0 at the US state level.





POTOMAC INSTITUTE FOR POLICY STUDIES  
901 N. Stuart St. Suite 1200, Arlington, VA 22203

[www.potomac institute.org](http://www.potomac institute.org)