UNITED KINGDOM
CYBER READINESS AT A GLANCE

Principal Investigator: Melissa Hathaway
Chris Demchak, Jason Kerben, Jennifer McArdle, Francesca Spidalieri

October 2016

POTOMAC INSTITUTE FOR POLICY STUDIES

Published by Potomac Institute for Policy Studies

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

Email: CyberReadinessIndex2.0@potomacinstitute.org

Follow us on Twitter:
@CyberReadyIndex

British flag on cover courtesy www.pixabay.com.
Cover art by Alex Taliesen.

Acknowledgements

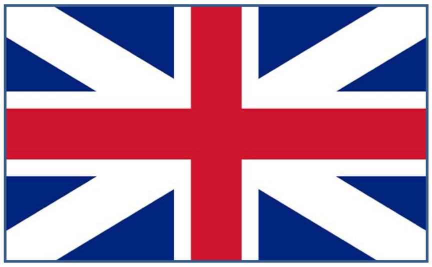
The Potomac Institute for Policy Studies and the authors would like to thank the following individuals for their contributions: Sir David Omand, GCB Visiting Professor in the Department of War Studies at King's College, London; and Paul Cornish, Oxford Martin Fellow at the Global Cyber Security Capacity Centre, University of Oxford. The authors would also like to thank Alex Taliesen for cover art and Sherry Loveless for editorial and design work.

UNITED KINGDOM
CYBER READINESS AT A GLANCE

TABLE OF CONTENTS

UNITED KINGDOM

CYBER READINESS AT A GLANCE



Country Population	64.6 million
Population Growth	0.8%
GDP at market prices (current $US)	$2.988 trillion
GDP Growth	2.3%
Year Internet Introduced	1991
National Cyber Security Strategy	2011
Internet Domain	.uk, .co.uk, .org.uk, .scot
Fixed broadband subscriptions per 100 users	37.4
Mobile broadband subscriptions per 100 users	123.6
Mobile phone subscriptions per 100 users	98.7

Information and Communications Technology (ICT) Development and Connectivity Standing

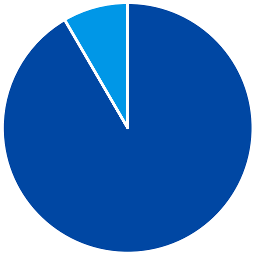
International Telecommunications Union (ITU) ICT Development Index (IDI)	4	World Economic Forum's Network Readiness Index (NRI)	8

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

INTRODUCTION

Commercial Internet was established in the United Kingdom (UK) in 1991 as part of a collaborative project between a US corporation (Oracle) and the British Telecommunication plc. (BT), formally government-owned. The following year, Pipex – the UK's first commercial Internet service provider (ISP) – introduced dial-up Internet service, providing Internet access to about 150 customer sites.

Since the early 1990s, connectivity has expanded exponentially, driving significant growth in e-government, e-commerce, and e-banking. Today, the UK is one of the most connected European countries with more than 90 percent Internet penetration – above the EU average of 79 percent.[1] In 2015, over 78 percent of Britons accessed the Internet on almost a daily basis, with over 74 percent of the population using Internet "on the go." The availability of wireless (WiFi) hotspots has been rapidly increasing and thousands of hotspots are now available across the country, including at pubs, cafes, hotels, etc. Mobile-broadband subscriptions have also more than doubled between 2010 and 2015, from 24 to 66 percent.[2]



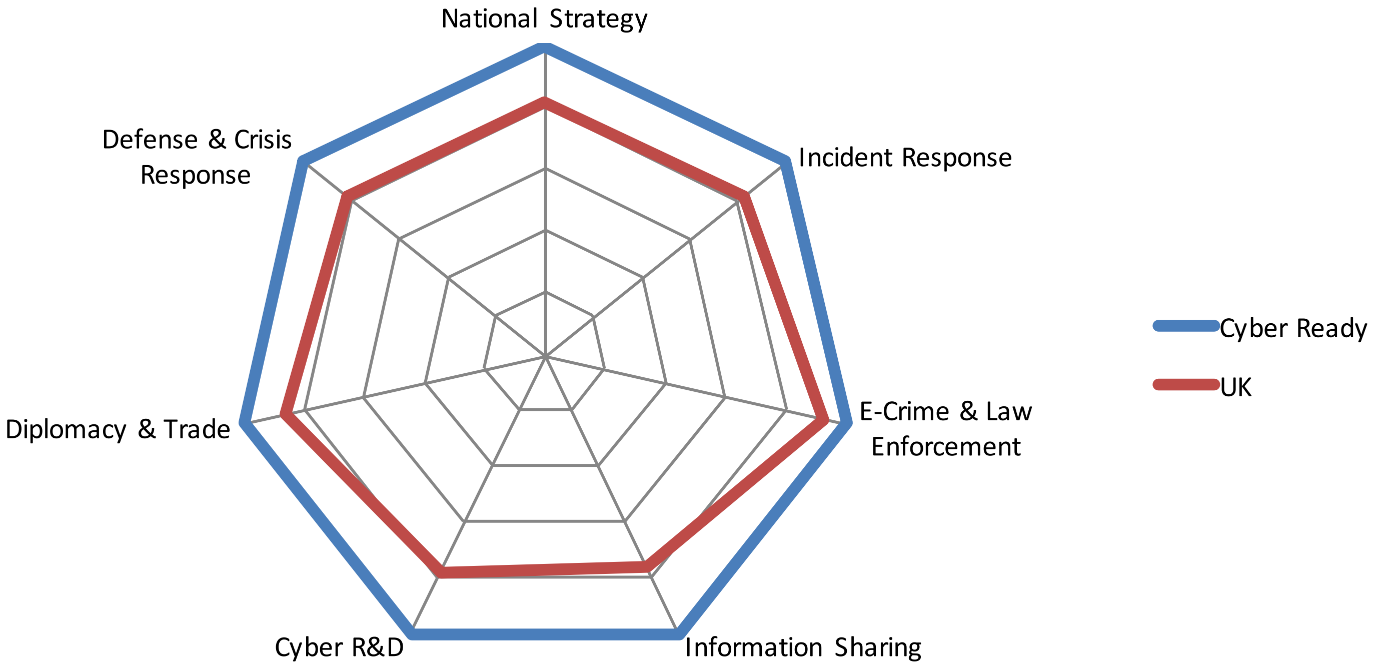
UK Internet Penetration: 91.6%

In 2013, the UK published a national digital strategy, the "Information Economy Strategy," with the aim of providing high-speed broadband access to enterprise zones and underserved communities.[3] Toward this end, Broadband Delivery UK (BDUK) – which forms part of the UK Department for Culture, Media and Sport – is implementing projects such as the Super Connected Cities Programme (SCCP) to support broadband growth in most cities. In addition, the digital strategy placed significant emphasis on ICT interoperability and standards, both within the UK communities and internationally. The UK has also taken a proactive stance on regulating the growing market influence of peer-to-peer (P2P) technologies, especially those influencing finance.[4]

As in many other developed countries, cyber security is a major challenge for the UK. In 2010, the British government recognized cyber security as a "Tier One risk"[5] to its economic and national security, and vowed to make the UK "the safest place to live and work online."[6] In 2011, former UK Foreign Secretary William Hague initiated the UK vision for safeguarding freedom and democratic values in cyberspace, forming the basis of future international agreements on norms of state behavior in cyberspace and outlined the key security priorities for the then-new British government. During his speech at the 2011 Munich Security Conference, he discussed all the steps that the British government had already taken to counter cyber threats, both domestically and internationally, and vowed to work with "the private sector to ensure secure and resilient critical infrastructure and the strong skills base needed to seize the economic opportunities of cyberspace, and to raise awareness of online threats among members of the public."[7] Despite these ambitious goals, various studies commissioned by the British government since then found that the theft of intellectual property is on the rise and that ever more UK organizations are falling victim to cyber incidents each year. The severity and impact of security breaches continue to grow as well, with an estimated cost for individual breaches in large organizations ranging between £600,000 and £1.15 million (between ~$741,363 and ~$1.42 million) as of 2015.[8]

The 2015 combined "National Security Strategy and Strategic Defence and Security Review" (SDSR) reiterated the Tier One level of national vulnerability and potential economic loss due to cyber insecurity.[9] In 2016, the UK's National Crime Agency (NCA) reported that cyber crime had surpassed all other forms of crime in the UK, and stressed the need for stronger law enforcement and business partnership to fight this threat.[10] As a result of the 2015 SDSR and subsequent reports on increasing volume and sophistication of cyber threats against UK's networks and information systems, the British government is planning to publish a new National Cyber Security Strategy in late 2016, and recently established a National Cyber Security Centre (NCSC) to serve as "the bridge between industry and government" to provide "a single point of contact for the private and public sectors alike."[11] In the accompanying second "National Cyber Security Programme," the British government plans to almost double its investment in cyber security – up to a maximum of £1.9 billion (~$2.35 billion) over the next five years. The Government Communications Headquarters (GCHQ) will play a leading role in the delivery of this strategic effort, and partnership with industry and academia has been recognized as "vital" for the success of the new center. The NCSC – which reports to and will act as the public-facing section of GCHQ – will provide authoritative advice on cyber security issues to businesses of all sizes and in all sectors in order to help them to better understand cyber threats and mitigate their impacts.[12]

The Cyber Readiness Index (CRI) 2.0 has been employed to evaluate UK preparedness levels for cyber risks. This analysis provides an actionable blueprint for the UK to better understand its Internet-infrastructure dependencies and vulnerabilities and assess its 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:



UK Cyber Readiness Assessment (2016)

1. NATIONAL STRATEGY

The 1st UK Cyber Security Strategy was published in 2009 and updated in 2011. The 3rd version is under development and may be released in late 2016.

The UK published its first national "Cyber Security Strategy" in 2009[13] and updated it in 2011.[14] Former UK Foreign Secretary William Hague outlined the key elements of the 2011 Cyber Security Strategy at the Munich Security Conference in February 2011. He asserted that "the Internet, with its incredible connective power, ha[d] created opportunity on a vast and growing scale; unlocking economic potential, revolutionizing access to information and requiring democratic governments to be more transparent." However, he also recognized that "there is a darker side to cyberspace that arises from our very dependency on it," and affirmed that: "Britain is ready to play its part" to combat cyber threats nationally and internationally.[15]

The 2011 strategy included a detailed description of cyber threats faced by the UK, and ranked cyber attacks and cyber crime as one of its top five priority risks. The accompanying implementation plan was based upon key targeted objectives, including fortifying the UK's cyber capabilities by establishing a new Defence Cyber Operation Group, and incorporating cyber security into the mainstream of British defense planning and operations. Since the publication of its second strategy, the British government has invested £860 million (~$1.06 billion) to accelerate the acquisition of new technology and capabilities to enable the execution of the 2011 "strategy's vision of a vibrant, resilient and secure cyberspace."[16] The strategy also designated the National Cyber Security Programme in the Cabinet Office as the competent authority with the responsibility to insure implementation of the strategy.

In addition, the UK national cyber security strategy synergizes UK national digital strategy (the 2013 "Information Economy Strategy"). Both documents recognize that while ICT is a key driver of economic growth, cyber security must underpin the information economy in order for such growth to be realized. As the UK digital strategy notes, "without [cyber security] businesses and consumers would not have the trust and confidence to use the Internet and other digital technologies."[17]

The National Cyber Security Centre (NCSC) will provide authoritative advice on cyber threats and help businesses mitigate their impacts.

The British government plans to invest up to £1.9 billion (~$2.35 billion) over the next five years to protect the UK from cyber attacks, and plans to release a second five-year national "Cyber Security Strategy" in late 2016, along with a subsequent five-year "National Cyber Security Programme." Finally, the newly established National Cyber Security Centre (NCSC) – headquartered in London with satellite offices at GCHQ in Cheltenham – aims to ensure the online safety of the general public, public and private sector organizations, as well as the UK's critical national infrastructure. The NCSC has four key objectives: (1) understanding the cyber security environment, sharing knowledge, and using this expertise to identify and address systemic vulnerabilities; (2) reducing cyber risk to British public and private sector organizations by providing guidance on effective mechanisms to improve their cyber security and conducting exercises; (3) responding to national cyber security incidents, through improved coordination of government and law enforcement activities; and (4) increasing national cyber security capability.[18] NCSC plans to have a staff of over 700 professionals by 2017, divided between the new London headquarters and GCHQ, and will include specialized teams for the City, Whitehall, intelligence and security services, energy, telecoms, and other critical national infrastructures.[19]

2. INCIDENT RESPONSE

Until 2014, the UK system for reporting and responding to cyber incidents was highly fragmented. There was no single national Computer Emergency Response Team (CERT), but rather two primary government CERTs that were focused on different organizational groups: (1) a Computer Security Incident Response Team (CSIRT-UK) set up under the Centre for Protection of National Infrastructure (CPNI) to serve companies in this sector; and (2) a GovCertUK to provide response services to government and wider public sector organizations. In accordance with the 2009 national Cyber Security Strategy, the British government also established a Cyber Security Operations Centre (CSOC), responsible for monitoring cyberspace and coordinating incident response.[20] In addition, the UK has over 20 other public and private CERTs and a dedicated Ministry of Defense CERT responsible for MOD networks.

In 2014, the UK established a Center for Cyber Assessment and the first UK's National CERT (CERT-UK) in accordance with the 2011 National Cyber Security Strategy. CERT-UK was tasked with four main responsibilities: handling national cyber security incident management; providing support to critical national infrastructure companies to handle cyber security incidents; promoting situational awareness of cyber security across industry, academia, and the public sector; and providing a single international point of contact for co-ordination and collaboration between national CERTs. The other CERTs were not dissolved, but CERT-UK became the primary national entity responsible for enhancing the UK's cyber resilience and ability to prepare for and manage national cyber security incidents. Their activities include: facilitating more effective domestic coordination of responses and information sharing (inclusive of an online reporting structure to log cyber security incidents); providing a contact and liaison point for international partners on trans-border incident response; participating in domestic exercises with government departments and industry partners (e.g., the "White Noise" exercise), and in multi-national cyber security exercises with NATO members; and collaborating with other national CERTs worldwide to build trust and enhance their understanding of cyber threats.

The first UK National CERT was established in 2014 in response to the 2011 National Cyber Security Strategy.

Moreover, CPNI and the National Technical Authority for Information Assurance (CESG, the Information Security arm of GCHQ) launched a pilot program and subsequently devised two Cyber Incident Response (CIR) schemes – a small government-run CIR one, and a more broadly-based one – to help critical national infrastructure companies obtain certified Cyber Incident Response services that are tailored to their needs, and to provide them with a list of companies that are certified to help respond to their specific incidents. This approach has enabled organizational victims of cyber attacks (including national and multinational industry, CNI, and the wider public sector and central government) to source appropriate incident response and streamline services that are tailored to their particular needs, while allowing GCHQ and CPNI to focus on those attacks that are the most challenging attacks to the nation. Another program recently launched by CESG – the "Certified Cyber Security Consultancy" scheme – certifies consultancy companies to provide security architecture, risk assessment, and risk management services to both the government and industry.[21]

The British government is working with CREST – a not-for-profit accreditation body that represents the technical information security industry – to assess the quality of suppliers of cyber security solutions and to approve vendors and products of cyber incident response, penetration testing, attack simulations, and other related programs. The Cyber Essentials program, for instance, was launched by CESG to both provide organizations with criteria and standards for basic cyber security, and help them better protect against cyber threats. Over 1,000 companies have already achieved Cyber Essentials certification status. As part of this program, CESG and CPNI have published highly successful guidance for industry that focuses on the practical steps that organizations can take to improve the security of their networks and mitigate or deter a majority of cyber attacks.[22] Taken together, the guidance document – published in 2012 and reissued in 2015, and entitled "10 Steps to Cyber Security" – and a set of best practices – published in 2015 and entitled "Small Businesses: What You Need to Know about Cyber Security"[23] – provide technical direction to businesses to help them increase their ability to reduce cyber risks. Other initiatives include a voucher scheme offering micro, small, and medium sized businesses up to £5,000 (~$6,178) to acquire specialist advice to strengthen their cyber security, protect new business ideas, and safeguard intellectual property.

Additionally, the Ministry of Interior is working with leading telecommunications companies to provide enhanced cyber security services to regulated critical infrastructures – especially within the financial, utility, communications, and transportation sectors. These services will give the British government increased visibility and understanding of specific cyber threats faced by these sectors – inclusive of both threats transmitted over and through the Internet, as well as those incurred by other means. In these ways, the program facilitates a more proactive defensive posture.

The new National Cyber Security Centre (NCSC) will be responsible for national cyber incident response and critical infrastructure protection.

The UK has conducted several national cyber security exercises in collaboration with industry to practice crisis response plans for government agencies and specific operators of critical infrastructure. For instance, in November 2013, the Bank of England conducted the "Waking Shark II Cyber Security Exercise" – a stress-test exercise developed to evaluate the response of the wholesale banking sector to a simulated cyber attack, as part of the ongoing work recommended by the UK Financial Policy Committee to assess and improve cyber resilience.[24] The British government actively collaborates with the US to organize exercises that test their respective financial sectors' incident response capabilities, and evaluate and reinforce cross-Atlantic coordination and communication mechanisms. In addition, the UK regularly participates in multi-national cyber security exercises, such as those organized by the European Union (EU), the NATO, the European Defense Agency (EDA) and the US Department of Homeland Security (e.g., Cyber Storm), with the goals of understanding cross-border dependencies and strengthening cyber incident response capacity among states.[25]

In addition to raising awareness of cyber threats and working with the business community and public sector to educate them on how best to stay safe online, the new National Cyber Security Centre (NCSC) is poised to become the competent authority responsible for national cyber security incident response and for ensuring the resilience of the UK's critical national infrastructure against cyber attacks. As part of this effort, CERT-UK functions are intended to be moved to NCSC, which will bring together the capabilities already developed by CESG, CPNI, and the Centre for Cyber Assessment in an effort to simplify the current arrangements and maximize British cyber capabilities.

3. E-CRIME AND LAW ENFORCEMENT

The UK Cyber Security Strategy 2011-2016 annual report reiterated the 2011 National Cyber Security Programme's commitment of "tackl[ing] cyber crime and mak[ing] the U.K. one of the most secure places in the world to do business in cyberspace."[26] Between 2011 and 2016, the British government allocated £860 million (~$1.06 billion) toward the cyber crime prevention initiative and three other cyber-related initiatives of the Programme.

Some of the notable efforts undertaken to address this overarching goal included the establishment of a new National Cyber Crime Unit (NCCU) in the National Crime Agency, which is responsible for coordinating the national response to the most serious cyber crime threats, and for supporting partners with specialist capabilities; and the establishment of a Cyber Unit in each of the nine Regional Organised Crime Units (ROCUs). NCCU receives funding from the National Cyber Security Programme, and works closely with ROCUs, the Metropolitan Police Cyber Crime Unit (MPCCU), and other partners within industry, government, and international law enforcement to respond to rapidly changing threats in a timely manner and reduce overall cyber crime.[27]

While the UK signed the Council of Europe Convention on Cybercrime (commonly known as the Budapest Convention) in 2001, actual ratification did not occur until just prior to a much-anticipated international cyber conference that was held in the UK – the 2011 London Conference on Cyberspace. In 2012, the UK's Foreign and Commonwealth Office invested £100,000 (~$123,560) to implement the requirements of the Budapest Convention in the UK.[28] Funding was dedicated to supporting workshops focusing on approaches to strengthening legislation related to cyber crime; training law enforcement agencies and the judiciary; and promoting public-private cooperation and international collaboration. According to the UK Cyber Security Strategy 2011-2016 annual report, the British government's Crown Prosecution Service (CPS) has also delivered training overseas to a variety of audiences including police, prosecutors, and judges on topics specifically related to e-crime and electronic evidence.[29]

The main applicable cyber crime law in the UK is the 1990 Computer Misuse Act, which makes unauthorized access to, or modification of computer material unlawful. In 2015, the Computer Misuse Act was amended by the Serious Crime Act 2015, which created a new offense for unauthorized acts that cause serious damage, implemented the EU Directive on Attacks against Information Systems, and clarified the savings provision for law enforcement agencies.[30]

Moreover, the NCA created a new national cyber crime unit, drawing together the work previously executed by the e-crime unit in Serious Organized Crime Agency (SOCA) and the Metropolitan Police's Central E-Crime Unit. The new unit performs the work of all four operational commands of the NCA (borders, organized crime, economic crime, and child exploitation and online protection (CEOP)) by providing specialist support, intelligence, and guidance. The unit acts as the national capability to deal with the most serious national-level cyber crimes, and part of the response to major national incidents.

4. INFORMATION SHARING

The Cybersecurity Information Sharing Partnership (CiSP), part of CERT-UK, was launched in 2013 as a joint, collaborative initiative between industry and government to share cyber threat and vulnerability infor-

The Cybersecurity Information Sharing Partnership (CiSP) is a private-public partnership to share cyber threat and vulnerability information.

mation in order to increase overall situational awareness and thus reduce the impact of cyber incidents upon UK business.[31] It is funded by the National Cyber Security Programme and brings together organizations of all sizes across a range of sectors. CiSP follows the goals and objectives set forth in the UK national cyber security strategy, and has grown exponentially in just three years to comprise over 2,220 organizations and 6,150 individuals, as of May 2016. The value of this collaboration has been recognized internationally, and CiSP has quickly become the de-facto standard for other countries, such as the Netherlands, which have established successful government-industry information sharing partnerships. CiSP members from across sectors and organizations, including CESG, law enforcement agencies, and international partners, can exchange cyber threat information in real time, in a secure and dynamic environment, while operating within a framework that protects the confidentiality of shared information. In addition, CiSP members receive regular cyber threat information, advisories, and alerts from the "Fusion Cell" – a joint industry and government analytical team that examines, analyzes, and gathers cyber threat information from a wide variety of data sources in order to help organizations at all levels of cyber maturity.[32] CiSP has also been involved in many of the national-level cyber security exercises, including the 2013 Waking Shark II.

CERT-UK has been housing CiSP and providing an international dimension to augment the day-to-day experience of working with critical national infrastructure companies in handling cyber incidents. Additional information exchange mechanisms, including non-profit research centers and membership organizations, have been established across the country.

The 2015 "National Security Strategy and Strategic Defence and Security Review" explicitly requires GCHQ to share cyber threat "knowledge with British industry and with allies."[33]

Finally, the new National Cyber Security Centre will serve as the authoritative source of information security in the UK and will act as a hub for sharing best security practices between the public and private sectors.[34] NCSC will run CiSP and its online platform, thus enabling a greater number of organizations to share important information both with each other and with the NCSC. The NCSC plans to use knowledge gathered from incidents and intelligence, together with that shared by other partners to provide best practice advice and guidance, to address systemic vulnerabilities, and to enhance the overall cyber security of the UK.

5. INVESTMENT IN RESEARCH AND DEVELOPMENT

The 2011 UK national cyber security strategy and the 2014 "Cybersecurity Strategy Report on Progress and Forward Plans" both communicate the British government's commitment to cyber security research and development (R&D).[35] Furthermore, the 2014 national innovation plan, entitled "Our Plan for Growth: Science and Innovation," established the British government's long term strategy to make the UK the "best place in the world for science and business."[36]

The GCHQ Cyber Accelerator is the first part of a renewed attempt by the UK government to invest in cyber security R&D.

UK investments in cyber R&D are overseen by several different government agencies, including: GCHQ, the new Department for Business, Energy and Industrial Reform (formerly the Department for Business, Innovation and Skills), the Department for Culture, Media and Sport (DCMS), the Cabinet Office, and the Engineering and Physical Sciences Research Council (EPSRC). As part of this commitment, in 2015, EPSRC provided £5 million (~$6.2 million) in funding to the Centre for Secure Information Technologies (CSIT) – the UK's knowledge and innovation center for cyber security research. The British government has also pledged to donate an additional £1.9 billion (~$2.35 billion) in funding by 2020 to cyber security research and innovation.[37] This set of investments is set to begin with the creation of a new GCHQ Cyber Accelerator as "the first step in the development of two world-leading innovation centres."[38] The new initiative aims to identify "companies that have developed novel techniques to solve real, existing cyber security problems, and digital companies whose products could be applied in a cyber security context."[39] The Department for Culture, Media and Sport has committed another £50 million (~$61.8 million) over the next five years to establish these two innovation accelerator centers.[40] The first Cyber Accelerator will be located in Cheltenham (where GCHQ is located) and is expected to open in early 2017. Companies selected to be part of this accelerator will also gain access to GCHQ staff and technology so as to understand the sort of cyber threats they face, and to expand capability, improve ideas, and devise cutting-edge products to combat current and emerging cyber threats. The second innovation center will open in London later in 2017. Both accelerators will be run by Wyra UK, part of Telefónica Open Future, which has been involved for a number of years in assisting other start-ups to develop ideas for innovation and growth.[41]

The UK faces a significant shortage of cyber security professionals who are able to protect the critical infrastructure and digital assets. It is estimated that in the UK, less than 0.6 percent of computer science graduates pursue careers in cyber security, and the UK's National Audit Office has warned that it could take up to 20 years to fill this skill gap in trained cyber security workers.[42] The UK Cabinet Office, the Department for Business, Energy and Industrial Reform, National Cyber Security Programme, and GCHQ are partnering to lead and support activities to increase cyber security skills at all levels of education. For example, the Cyber Security Challenge UK – a not-for-profit organization supported by the British government, industry, and academia – runs national competitions designed to attract and inspire yet untapped cyber security talent, and organizes cyber camps to help people develop new skills and explore cyber security-related career opportunities.[43] "CyberFirst," one of the latest GCHQ initiatives, is designed to identify and train young talent with different backgrounds to support GCHQ and the UK's cyber security mission. Selected individuals are offered sponsorship to pursue cyber-relevant undergraduate degrees, practice cyber skills during summer internships, and ultimately, work in the national security sector upon graduation.[44]

In 2016, the British government published a report entitled, "Cyber Security: Programmes and Resources for Schools and Further Education," which sought to provide guidance for teachers to better integrate cyber security into their curricula. In addition, GCHQ provides criteria for a specific GCHQ Certified Master's degree in Cyber Security. To date, ten UK universities have met the rigorous standard to deliver GCHQ Certified Master's degrees in General Cyber Security, and other large UK universities offer degree programs in cyber security at the masters and doctoral levels, including the University of Birmingham, University of Bristol, University of Cambridge, Imperial College London, Lancaster University, among others. Eleven other universities in the UK have gained the status of "Academic Centres of Excellence" in recognition of their high standard of cyber security research and efforts. These Academic Centers have partnered with private sector companies, such as Google and Mozilla, to develop new cutting edge cyber security solutions to issues like privacy protection, and have also developed collaborations with other countries to promote cyber security research and development.[45]

In 2010, the British government established the "Catapult Programme" – a network of world-leading centers designed to harness UK innovation and help drive future economic growth by bringing together UK businesses, scientists, and engineers to work side by side on late-stage research and development.[46] The program had an initial investment of £200 million (~$247 million) and was intended to be a new force for innovation and growth for the UK. It aimed to connect businesses with the UK's research and academic communities to work collaboratively on solving key problems and transform high-potential ideas into new products and services that can be sold on a broad commercial scale. The first Catapult centers are transforming British efforts in innovation by concentrating expertise, enabling access to cutting-edge equipment, and establishing specialist facilities to develop and test ideas and translate concepts into products and services.

The UK also participates in the EU's "Horizon 2020" program, which has as one of its principal aims to enhance collaboration between the private and public sectors through groundbreaking R&D in order to generate growth in the ICT sector.[47] Additionally, London's "cyber innovation hubs" – Cyber London or CyLon – was Europe's first cyber security accelerator and incubator space, which was developed to foster cyber innovation and help businesses develop information security-related products.[48]

The NCSC will also play a leading role in addressing critical national cyber security issues by bringing together government, industry, and academic entities to harness the advantages of ICTs, understand systemic vulnerabilities through root cause analyses, and work with key stakeholders and incentivize the market to better address those cyber threats.

6. DIPLOMACY AND TRADE

The UK launched the "London Process" – bringing countries together to address norms of acceptable behavior in cyberspace.

The UK has been a pioneer in the development and promotion of international norms in cyberspace, and in the engagement of a variety of stakeholders in international discussions on cyber security, cyber crime, economic growth and development, and Internet governance. In 2011, former UK Foreign Minister William Hague convened the London Conference on Cyberspace – the first of a series of inter-ministerial gatherings hosted by countries around the world that have since become known as the "London Process." Underlying these thematic conversations has been the goal of bringing more countries together to address the need for both better-articulated norms of acceptable behavior in cyberspace, and a commitment to work collaboratively to protect the potential and security of the Internet. Minister Hague highlighted key principles that should "underpin future international norms about the use of cyberspace" during his remarks at the 2011 Munich Security Conference.[49] These tenets included the principle of proportionality in cyberspace in accordance with national and international law; the right for everyone to have the ability – in terms of skills, technology, confidence, and opportunity – to access cyberspace; the protection of the freedom of expression, opinion, privacy, and intellectual property; a respect for diversity of language, culture, and ideas; the need to collectively fight cyber crime; and the promotion of a competitive environment that insures a fair return on investment in networks, services, and content.[50]

These foundational elements, coupled with a multi-stakeholder approach, became the basis of many cyber-related agreements reached by the United Nations Group of Governmental Experts (UN GGE), in which the UK has played an active role in recent years. In July 2015, the UN GGE reaffirmed conclusions reached in 2013 that international law – especially the UN Charter – applies in cyberspace.[51] They also agreed to a new report on how international law may apply in cyberspace, and made recommendations on confidence-building measures (CBMs), international cooperation, and capacity building.[52] The voluntary, non-binding norms of responsible state behavior in cyberspace proposed in this report were ultimately adopted by the UN General Assembly in December 2015, and were later endorsed by the G-20.

The UK is also a member of the Organisation for Security and Co-operation in Europe (OSCE), and has been an active participant in discussions that led to two major agreements on additional CBMs in the field of cyber security and use of ICTs. The first agreement – the OSCE Decision 1106 – was reached in December 2013 and outlined eleven specific CBMs aimed at enhancing interstate co-operation, transparency, predictability, and stability, and reducing the risks of misperception, escalation, and conflict that may stem from the use of ICTs.[53] The OSCE Decision 1202, agreed upon in March 2016, re-affirmed the original eleven CBMs and added five more measures specifically designed to reduce the risks of conflict stemming from the use of ICTs.[54] These measures focused on the need to protect communications' channels to reduce the risk of misperception and escalation; to develop shared crisis management procedures in case of widespread or transnational disruption of ICT-enabled critical infrastructure; to develop means to exchange best practices; to improve the security of national and trans-national ICT-enabled critical infrastructure including their integrity at the regional and sub-regional levels; and to encourage responsible reporting of vulnerabilities affecting the security of and in the use of ICTs.

Some notable bilateral engagements have included a UK cyber security trade mission to Israel in February 2016, which has strengthened business and academic collaboration between the two countries, including in research and CERT-to-CERT co-operation on incident management. In 2015, the India-UK Cyber Dialogue and Prime Minister Modi's visit to the UK served to strengthen ongoing collaboration on cyber issues. Both countries reaffirmed their commitment to combating cyber crime, advancing voluntary norms of responsible state behavior, and applying international law in cyberspace.[55] In addition, the UK and China have had a successful Track 1.5 Dialogue on Cyber Security since 2013, which has helped to identify and foster collaboration in areas where UK and Chinese policies and interests coincide, while also clarifying those areas where differences in perception are not aligned.[56]

The British government has also developed industry-led standards to promote the UK as "a safe place for internet trade and commerce," and to assist "U.K. businesses to promote their products or services within both domestic and overseas markets."[57] For example, the Cyber Essentials program, launched by CESG in 2014, has helped organizations of all sizes and in all sectors to develop cyber security criteria and standards to be better protected from the most common cyber threats. Cyber Essentials' requirements and standards are applicable to academic, private, and public sector organizations alike.[58]

In December 2015, the UK assisted with securing informal agreement on the draft EU Network and Information Security (NIS) Directive to improve cyber security capabilities and cooperation across Europe. The NIS Directive was formally adopted by the European Council in May 2016 and entered into force in August 2016.[59] Despite the UK vote to leave the EU – i.e., "Brexit" – in June 2016, the country may still be bound to comply with this directive and other EU data protection and data privacy regulations, at least until the UK's withdrawal from the EU is formalized. At present, UK firms trading with EU member states will need to comply with the new European General Data Protection Regulation (GDPR) when it is enacted in 2018. Since both the NIS and GDPR regulations have already been finalized, many international businesses headquartered in the UK will also be impacted, and some are even considering leaving the UK for "European" soil. This may force the UK to negotiate independent data privacy and security agreements with the EU, or to adopt national legislation that is aligned with EU regulations in order to continue trade and business operations in EU markets.[60]

7. DEFENSE AND CRISIS RESPONSE

The 2015 combined "National Security Strategy and Strategic Defence and Security Review" clearly identified GCHQ as the primary governmental organization with the national responsibility "to develop capability, to detect and analyze cyber threats, pre-empt attacks, and track down those responsible."[61] In the same document, the Ministry of Defense asserted its intention to develop a "Joint Cyber Group" to coalesce its cyber capabilities to defend MOD's military defense networks (primarily), while also assisting the defense of the whole-of-nation as needed. The British government has stated a willingness to employ non-cyber punitive responses to major cyber attacks on national assets and interests, which would presumably involve GCHQ and military capabilities as required, and has even discussed the possibility to consider "active cyber defense" that is in line with the government's stated intention to make the UK the "best protected country in cyberspace."[62]

The UK intends to be the best protected country in cyberspace.

Along with the NCSC, the British government has pledged £40 million (~$49 million) to open a new Cyber Security Operations Centre (CSOC) under the guidance of the GCHQ in order to better share critical cyber-related intelligence and forensics with key agencies and other actors across the UK.[63] The move is part of a larger effort by the government to develop and utilize "state-of-the-art" defensive cyber security tactics, to improve the UK's ability to protect against threats to defense networks and systems, and to develop sovereign capabilities in cyberspace. The CSOC initiative will provide support to British armed forces and help strengthen the UK's cyber security posture overall (i.e., via coordination of government departments, industry, and international partners).

As consistent with its long, established membership in NATO, the UK regularly participates in NATO cyber exercises, planning, and operations. It also participates in other smaller regional, allied, and bilateral cyber-related defense exercises with other countries, within the EU and abroad. While results of these exercises relative to the overall effectiveness of the UK's larger systemic cyber defense are not publicly known, GCHQ and the UK MOD are routinely grouped with the small number of EU nations that are considered to have the most advanced defense cyber capacity.

CRI 2.0 BOTTOM LINE

According to the CRI 2.0 assessment, the UK 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 about the UK's cyber preparedness and capability. As the UK continues to develop and update its economic (digital agenda) and national 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.potomacinstitute.org/academic-centers/cyber-readiness-index.

Legend

● Fully Operational

◐ Partially Operational

○ Insufficient Evidence

IDI Rank		NRI Rank	GDP Rank	National Strategy	Incident Response	E-Crime & Law Enforcement	Information Sharing	Investment in R&D	Diplomacy & Trade	Defense & Crisis Response
4	United Kingdom	8	5	◐	◐	◐	◐	◐	◐	◐

ENDNOTES

1. World Bank, “Internet Users (per 100 people),” 2014, http://data.worldbank.org/indicator/IT.NET.USER.P2.

2. UK Office for National Statistics, “Internet Access – Households and Individuals: 2015,” August 6, 2015, http://www.ons.gov.uk/peoplepopulationand-community/householdcharacteristics/homeinternetandsocialmediausage/bulletins/internetaccesshousehold-sandindividuals/2015-08-06.

3. UK Department for Business, Innovation and Skills, “Information Economy Strategy,” June 14, 2013, https://www.gov.uk/government/publications/information-economy-strategy.

4. OECD, “OECD Digital Economy Outlook 2015,” July 15, 2015, http://www.oecd.org/internet/oecd-digital-economy-out-look-2015-9789264232440-en.htm.

5. UK Government, “Securing Britain in an Age of Uncertainty: The Strategic Defence and Security Review, (2010): 47, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/62482/strategic-defence-security-review.pdf.

6. UK Parliament, “Final Annual Report on the 2011-2016 UK Cyber Security Strategy,” April 14, 2016, http://www.parliament.uk/business/publications/written-questions-an-swers-statements/written-statement/Lords/2016-04-14/HLWS652/.

7. UK Government, “Foreign Secretary William Hague’s Speech at the Munich Security Conference: Security and Freedom in the Cyber Age – Seeking the Rules of the Road,” February 4, 2011, https://www.gov.uk/government/speeches/security-and-freedom-in-the-cyber-age-seeking-the-rules-of-the-road.

8. UK Government, “PwC 2015 Information Security Breaches Study on UK Corporations,” (2015), https://www.pwc.co.uk/assets/pdf/2015-isbs-tech-nical-report-blue-03.pdf.

9. UK Government, “National Security Strategy and Strategic Defence and Security Review,” (2015), https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/478933/52309_Cm_9161_NSS_SD_Review_web_only.pdf.

10. National Crime Agency, “Cyber Crime Assessment 2016,” http://www.nationalcrimeagency.gov.uk/publica-tions/709-cyber-crime-assessment-2016/file.

11. UK Government, “Prospectus: Introducing the National Cyber Security Centre,” May 25, 2016, https://www.gov.uk/government/publications/national-cyber-security-centre-prospectus.

12. “National Cyber Security Centre HQ Operational,” *SC Magazine UK*, October 3, 2016, http://www.scmagazineuk.com/ncsc-will-be-based-in-the-nova-office-and-shopping-com-plex-near-victoria-station-in-london/article/526405/.

13. UK Cabinet Office, “Cyber Security Strategy of the United Kingdom,” (June 2009), https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/228841/7642.pdf.

14. UK Cabinet Office and National Security and Intelligence, “Cyber Security Strategy,” November 25, 2011.

15. UK Government, “Foreign Secretary William Hague’s Speech at the Munich Security Conference: Security and Freedom in the Cyber Age – Seeking the Rules of the Road.”

16. UK Government, “UK Cyber Security Strategy: Statement on the Final Annual Report,” April 14, 2016, https://www.gov.uk/government/speeches/uk-cyber-security-strategy-statement-on-the-final-annual-report.

17. UK Government, “Information Economy Strategy,” (June 2013).

18. UK Government, “Prospectus: Introducing the National Cyber Security Centre,” (March 2016): 4.

19. “National Cyber Security Centre HQ operational,” *SC Magazine UK*.

20. UK Cabinet Office, “Cyber Security Strategy of the United Kingdom,” 5.

21. Rene Millman, “GCHQ Information Security Arm CESG Awards Six Firms Certified Cyber Security Consultancy Status,” *Public Technology*, February 15, 2016, https://www.publictechnology.net/articles/news/gchq-information-security-arm-cesg-awards-six-firms-certified-cyber-security.

22. GCHQ, “Re-Launch of ’10 Steps to Cyber Security’,” January 16, 2015, https://www.gchq.gov.uk/news-article/re-launch-10-steps-cyber-security.

23. UK Government, “Small Businesses: What You Need to Know about Cyber Security,” March 2015, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/412017/BIS-15-147-small-businesses-cyber-guide-March-2015.pdf.

24. UK Government, “Government and Regulators Meet to Combat Cyber Threats to Essential Services,” February 5, 2014, https://www.gov.uk/government/news/government-and-regulators-meet-to-combat-cyber-threats-to-essential-services.

25. European Defense Agency, “Complex Cyber Crisis Management Exercise in Vienna,” September 16, 2015, https://www.eda.europa.eu/info-hub/press-centre/latest-news/2015/09/16/complex-cyber-crisis-management-exercise-in-vienna, and NATO, “Largest Ever NATO Cyber Defence Exercise Gets Underway,” November 21, 2014, http://www.nato.int/cps/en/natohq/news_114902.htm?selectedLocale=en.

26. UK Cabinet Office, "The UK Cyber Security Strategy 2011-2016: Annual Report," (2016): 5, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/516331/UK_Cyber_Security_Strategy_Annual_Report_2016.pdf.

27. National Crime Agency, "National Cyber Crime Unit," http://www.nationalcrimeagency.gov.uk/about-us/what-we-do/national-cyber-crime-unit.

28. "UK Gives £100K to Implement Convention on Cybercrime," *Information Age*, March 2, 2012, http://www.information-age.com/technology/security/2089928/uk-gives-£100k-to-implement-convention-on-cybercrime.

29. UK Cabinet Office, "The UK Cyber Security Strategy 2011-2016: Annual Report," (2016): 13.

30. UK Government, "Serious Crime Act 2015," March 2015, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/415953/Factsheet_-_Computer_Misuse_-_Act.pdf.

31. CERT-UK, "Cybersecurity Information Sharing Partnership (CiSP)," https://www.cert.gov.uk/cisp/.

32. CERT-UK, "Fusion Cell," https://www.cert.gov.uk/cisp/.

33. UK Government, "National Security Strategy and Strategic Defence and Security Review," (2015): 40.

34. John Leyden, "National Cyber Security Centre to Shift UK to 'Active' Defence," *The Register*, September 16, 2016, http://www.theregister.co.uk/2016/09/16/uk_gov_active_cyber_defence/.

35. UK Cabinet Office, "The UK Cyber Security Strategy Report on Progress and Forward Plans," (2014): 23.

36. UK Department for Business, Innovation & Skills, "Our Plan for Growth: Science and Innovation," (2014): 5, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/387780/PU1719_HMT_Science_.pdf.

37. EPSRC, "EPSRC and Innovate UK Announce £5 Million Investment in UK Cybersecurity Research and Innovation," March 19, 2015, https://www.epsrc.ac.uk/newsevents/news/csit1/, and David Crozier, "CSIT Labs is Launched: An Incubator Programme Designed to Engineer Viable Ventures in Cyber Security," CSIT Labs, November 24, 2015, https://www.csitlabs.com/2015/11/24/csit-labs-is-launched-an-incubator-programme-designed-to-engineer-viable-ventures-in-cyber-security/.

38. GCHQ Cyber Accelerator, "Developing the UK's Cyber Security Ecosystem Through the Acceleration of Innovative Cyber Security Start-ups," https://wayra.co.uk/gchq/.

39. *Ibid.*

40. Dan Worth, “Government, GCHQ and O2 Team up to Create Cyber Security Startup Labs,” *V3*, September 23, 2016, http://www.v3.co.uk/v3-uk/news/2471833/government-gchq-and-o2-team-up-to-create-cyber-security-startup-labs.

41. Matt Burgess, “GCHQ Launches Cyber Security Accelerator with Wayra,” *Wired*, September 26, 2016, http://www.wired.co.uk/article/gchq-wayra-cyber-startup-accelerator.

42. Sean Coughlan, “Cyber-attacks Increase Leads to Jobs Boom,” March 26, 2014, *BBC News*, http://www.bbc.com/news/business-26647795.

43. CESG, “Cyber Security Challenge,” October 17, 2015, https://cybersecuritychallenge.org.uk/education/insights-camps/.

44. GCHQ, “Investing in Cyber,” June 3, 2016, https://www.gchq.gov.uk/features/investing-cyber.

45. UK Cabinet Office, “The UK Cyber Security Strategy Report on Progress and Forward Plans,” (2014): 23.

46. Catapult, “About Us,” https://www.catapult.org.uk/about-us-text.

47. UK Government, “Innovate UK: Emerging and Enabling Technologies,” April 7, 2016, https://www.gov.uk/government/collections/innovate-uk-emerging-and-enabling-technologies, and “Horizon 2020: What It Is and How to Apply for Funding,” November 3, 2015, https://www.gov.uk/guidance/horizon-2020-what-it-is-and-how-to-apply-for-funding.

48. “CyLon,” https://cylonlab.com.

49. UK Government, “Foreign Secretary William Hague’s Speech at the Munich Security Conference: Security and Freedom in the Cyber Age – Seeking the Rules of the Road,” February 4, 2011, https://www.gov.uk/government/speeches/security-and-freedom-in-the-cyber-age-seeking-the-rules-of-the-road.

50. *Ibid*.

51. US Department of State, “Statement on Consensus Achieved by the UN Group of Governmental Experts on Cyber Issues,” *Press Release*, June 7, 2013, http://www.state.gov/r/pa/prs/ps/2013/06/210418.htm.

52. NATO CCDCOE, “2015 UN GGE Report: Major Players Recommending Norms of Behaviour, Highlighting Aspects of International Law,” August 31, 2015, https://ccdcoe.org/2015-un-gge-report-major-players-recommending-norms-behaviour-highlighting-aspects-international-l-0.html.

53. OSCE, “Permanent Council Decision No. 1106,” December 3, 2013, http://www.osce.org/pc/109168.

54. OSCE, “Permanent Council Decision No. 1202,” March 10, 2016, http://www.osce.org/pc/227281.

55. UK Cabinet Office, “The UK Cyber Security Strategy 2011-2016: Annual Report,” (2016): 15.

56. International Institute for Strategic Studies, “Sino-UK Track 1.5 Dialogue on Cyber Security,” October 15, 2014, https://www.iiss.org/en/about%20us/press%20room/press%20releases/press%20releases/archive/2014-dd03/october-a29d/sino-uk-track-15-dialogue-on-cyber-security-1496.

57. UK National Audit Office, “The UK Cyber Security Strategy: Landscape Review,” (February 2013): 25, http://www.nao.org.uk/wp-content/uploads/2013/03/Cyber-security-Full-report.pdf.

58. UK Government, “Cyber Essentials Scheme: Overview,” April 7, 2014, https://www.gov.uk/government/publications/cyber-essentials-scheme-overview.

59. European Council, “EU-wide cybersecurity rules adopted by the Council,” May 17, 2016, http://www.consilium.europa.eu/en/press/press-releases/2016/05/17-wide-cybersecurity-rule-adopted/.

60. Mark Rasch, “Brexit’s Potential Impact on Information Security,” *Security Current*, June 27, 2016, http://www.securitycurrent.com/en/ciso_journal/ac_ciso_journal/brexits-potential-impact-on-information-security.

61. UK Government, “National Security Strategy and Strategic Defence and Security Review.”

62. UK Government, “Chancellor’s speech to GCHQ on cyber security,” November 17, 2015, https://www.gov.uk/government/speeches/chancellors-speech-to-gchq-on-cyber-security.

63. This new agency replaces an earlier, Cabinet-led, multi-agency version defined by the 2011 U.K. Cyber Security Strategy and set up in 2012. The new Cyber Security Operation Centre is intended to have a more effective relationship between the computer intelligence expertise at GCHQ and the audiences it is supposed to serve. For more on the new CSOC, see: U.K. Government, “Defence Secretary Announces £40 million Cyber Security Operations Centre,” April 1, 2016, https://www.gov.uk/government/news/defence-secretary-announces-40m-cyber-security-operations-centre.

For more information or to provide data to the CRI 2.0 methodology, please contact:
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.

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.potomacinstitute.org