# The British Response to Threats in Cyberspace

Daniel Cohen

The cyber threat ranks high among the risks to a country's interests and national security. In recent years, this threat has already materialized in cyberattacks on political institutions, political parties, organizations, financial institutions, and critical national infrastructure around the world. In the future, additional risks are expected, particularly to the civilian sector, originating in the Internet of Things. These risks are the result of the growing number of connected devices, most of which are neither secured by the manufacturers nor by the users, and the rise in the number of Denial-of-Service (DoS) attacks on public and private systems that are accompanied by extortion and ransom demands.

This article focuses on cybersecurity efforts in Britain. The inherent gaps between characteristics of the flexible and dynamic British private sector and the needs of the bureaucratic and innately sluggish secret security system have hindered collaborative efforts between the cyber industry in Britain and the security system there, as well knowledge sharing between sectors as is needed today. In response to this situation, the government has undertaken strategic processes in recent years to support subjects relating to technology and innovation, with an emphasis on knowledge-intensive industry and cybersecurity. The objective of these processes has been to contend with the changing dynamics of the cyber threats, while attempting to build a bridge between the British intelligence

Daniel Cohen is a researcher in the Yuval Ne'eman Workshop for Science, Technology and Security and in the Blavatnik Interdisciplinary Cyber Research Center, Tel Aviv University.

agencies and the private market, in relation to issues of defense, research, and development.

**Keywords**: Cyber security, Britain, research and development, cyber defense, GCHQ, NCSC, deterrence, international cooperation

## Introduction

Britain has a long history of using science and technology for the purposes of national security, and its governments have maintained long-range strategies and policies over the years to support the fields of innovation, technology, and knowledge-intensive industry. The Signals Intelligence Corps (SIGINT), which operated on behalf of the British War Ministry, engaged in intercepting the Germans' transmissions during World War I, while sharing knowledge with their French counterparts. British decoding and intelligence collection efforts expanded considerably during World War II and in 1945, approximately 10,000 employees served in the SIGINT service in Bletchley Park.[1]

The British Government Communications Headquarters (GCHQ) was established during the Cold War and is responsible for SIGINT and technology, cyber, and additional tasks related to Britain's national security. Concurrently, the GCHQ provides guidance to government organizations and critical infrastructure organizations in relation to information systems security. In addition to various operative departments, an advanced research department operates in the GCHQ and engages in a variety of topics, such as network architecture, security, linguistics, artificial intelligence, automated machines, and more.

In 2013, the GCHQ was the focus of public discourse, following the publication of the intelligence commissioner's report on behalf of the British government, which contained recommendations for reforms, new legislation, and processes for regulating possible surveillance and wiretapping by British intelligence and the police. This report emphasized the need to create a bridge between the British intelligence agencies and the private market in relation

1 See Government Communications Headquarters (GCHQ) website, https://www.gchq-careers.co.uk/about-gchq.html.

to issues of defense, knowledge sharing, and research and development.[2] As part of the restructuring, which was designed to create national cybersecurity capability in the civilian sector, the British government announced the establishment of the National Cyber Security Center (NCSC) in November 2015. The center is to be subordinate to the GCHQ but will bear state responsibility for providing cybersecurity to the entire British society and will constitute an address for advice and support for the economic system, while directly cooperating with academia and international entities. The intention of the British government was to render the security system that contends with cyber threats more accessible and capable of cooperating with the private sector in order to share knowledge and resources.[3]

## British Government Funding of Technological Research and Development

Over the last three decades, the British government has reduced its investments in research and development. In 2012, for example, the investments in research and development were about 1.72 percent of the British GDP, compared to about 2 percent of the GDP at the end of the 1980s. This figure is also lower than the average of EU member states, which was 2.06 percent in 2012.[4] In 2014, the British government set a target increase in state investments in research and development to 3 percent of the GDP by the year 2020.[5]

Today, the majority of investments in technology and innovation in Britain are allocated to encourage the private sector and not the public sector. The government budgeting for science and research reaches about GBP 4.6

2 Intelligence Services Commissioner, *Report of the Intelligence Services Commissioner for 2013*, June 26, 2014, http://intelligencecommissioner.com/docs/40707_HC304IntelligenceServicesCommissioner_Accessible.pdf.

3 Royal Society, *Progress and Research in Cybersecurity: Supporting a Resilient and Trustworthy System for the UK*, (The Royal Society, July 2016), p. 37, https://royalsociety.org/~/media/policy/projects/cybersecurity-research/cybersecurity-research-report.pdf.

4 Charlie Edwards and Calum Jeffray, "The Future of Research and Development in the UK's Security and Intelligence Sector," (Occasional Paper, Royal United Services Institute, March 2015), https://rusi.org/publication/occasional-papers/future-research-and-development-uk%E2%80%99s-security-and-intelligence-sector.

5 National Audit Office, *Research and Development Funding for Science and Technology in the UK*, Memorandum for the House of Commons Science and Technology Committee, June 2013, p. 7.

billion per annum and does not include direct allocations to the security sector (in which there have been budget cuts since 2010). Between 2010–2014, the digital industries in Britain grew by about 32 percent—faster than the British economy—and employment in these industries increased by 2.8 percent, faster than in all other sectors of the economy. In 2015, 86 percent of the households in the country had internet connections and 76 percent shopped online. In 2016, about 56 percent of the adult population in Britain used a digital bank. Today, the digital industry in Britain constitutes about 7 percent of the British economy and employs 5 percent of the workforce.[6] Notwithstanding the increased use of digital space, the British economy has suffered from rising unemployment rates among technology professionals, while, on the other hand, it has a shortage of professionals in the cyber field.[7] The government identified this gap and today aims to deepen the cooperation between the GCHQ and British industry and to contribute to the growth of the cyber market. The value of this market is currently assessed to be about GBP 22 billion, but revenue from exports of cyber products account for only GBP 2 billion.[8]

Due to the threats in cyberspace, the British government in 2011 formulated a National Cyber Security Strategy for 2011–2016 that reflected the need to create an efficient ecosystem in which the government, the security system, academia, industries, and start-up companies would collaborate in order to respond to the growing security needs. Within this framework, the government decided to invest GBP 860 million in the development of a national cyber security plan.

The implementation of this new strategy was reflected initially by establishing cybersecurity bodies, such as the national Computer Emergency Response Team (CERT), creating platforms for knowledge sharing, encouraging cyber studies in academia, and delegating responsibilities among the various bodies in charge of cyber security. Despite some successes, this strategy was

6 Office for National Statistics, *Internet Access – Households and Individuals: 2015*, http://www.ons.gov.uk/peoplepopulationandcommunity/householdcharacteristics/ homeinternetandsocialmediausage/bulletins/internetaccesshouseholdsandindividuals/2015-08-06.

7 "Jammin' in the Capital," *Economist*, June 21, 2014, http://www.economist.com/news/britain/21604591-londons-creative-talents-have-unleashed-wave-innovative-technology-firms-jammin.

8 Ibid.

unsuccessful in closing the structural gaps between the flexible and dynamic private sector and the needs of the bureaucratic and innately sluggish secret security system. The lack of systemic transparency also impaired efficiency in the cooperative efforts between industry and the security system in Britain and the knowledge sharing between the sectors. During these years, the British national cyber budget was mostly invested in developing state cybersecurity capabilities, including channeling budgets to law-enforcement agencies that were battling organized crime. Relatively smaller budgets were allocated to the private sector, academia, and the education system.[9]

## Updating Britain's National Cyber Strategy

The British National Security Strategy, which was published in 2015, defined the cyber threat as one of the most critical threats and as one of the highest risks to British interests.[10] One year later, Britain's National Cyber Strategy for 2016–2021 was published. This document defined cybersecurity as "protection of information systems (software, hardware and related infrastructure), the information contained in these systems and the services that the systems provide, against intrusion by unauthorized parties, damage or improper use, including premeditated damage caused by a system operator, or unintentional damage resulting from noncompliance with security regulations."[11]

The National Cyber Strategy identified the following main threats to British cyberspace:[12]

- **Cybercrime**: Cyber-based crimes are committed using Information and Communications Technology (ICT), when both the attacker and the victim are using ICT tools; the development of malware to commit financial scams, burglary, theft, disruption or deletion of information; "traditional" crimes in which criminals are aided by computers, computer networks,

9 About three-quarters of the national cyber budget for 2011–2016, which totaled GBP 650 million, were allocated to the GCHQ and to additional security agencies. See National Audit Office, *The UK Cyber Security Strategy: Landscape Review*, February 12, 2013, p. 16, https://www.nao.org.uk/wp-content/uploads/2013/03/Cyber-security-Full-report.pdf.

10 *National Security Strategy and Strategic Defense and Security Review 2015*, November 23, 2015, Cm. 9161, https://www.gov.uk/government/publications/national-security-strategy-and-strategic-defence-and-security-review-2015.

11 HM Government, *National Cyber Security Strategy* 2016–2021, p. 15.

12 Ibid, p. 18.

or any other type of ICT (such as information theft or fraud); organized cybercrime by criminal organizations, with an emphasis on Russian-speaking organizations based in Eastern Europe.

- **Countries and state-sponsored groups**: There are repeated attempts by groups to infiltrate British information networks who seek to achieve strategic, political, technological, and commercial advantages. The main threats in this context are to government, security, economic, energy, and communications bodies. Only a limited number of countries have the capability to pose a serious threat to Britain, although many other countries are in the process of developing (or purchasing) cyber tools that could pose a threat to Britain in the not-too-distant future. In addition to espionage campaigns, there is a threat of attacking critical infrastructure.
- **Terrorist attacks**: Terrorist groups are conducting activities in cyberspace against British targets, even though their technical capabilities are poor at this stage; nevertheless, even attacks using simple tools have the potential to cause tremendous damage. Most of the threats are website defacement attacks, leaking personal information, and so forth as the objective of the terrorist organizations is to achieve public exposure and to intimidate victims. The frequency of DoS attacks and website defacements are forecasted to rise, coupled with an increased use of insider threats.
- **Hacktivism**: These are groups of activists whose principal attacks are DoS and website defacement. These groups are decentralized and focus their attacks on specific issues and carefully choose their victims.
- **Script kiddies**: These are individuals with limited cyber capabilities who use attack tools developed by others. They do not have the potential to pose a wide-scale threat to the economy and society but do have the potential to cause significant damage to an individual or to an organization.

The British cyber strategy published in 2011 did not achieve the target of securing Britain's digital assets. This situation led the British government to understand that it needed to invest more substantial resources to contend with the changing dynamics of the threats and resulted in the drafting of its vision for 2021, which relies on the approach of the National Cyber Security Strategy. This approach includes four key components: defense, deterrence, development, and international activity, as specified below:[13]

13 Ibid., p. 15.

**Defense:** Defense is based on the existing resources in Britain for defending against cyber threats, with the objective of creating an effective response capability and ensuring the proper functioning of networks and information systems. The basic assumption is that Britain must reach its objective, whereby civilians, businesses, and the public service will have the know-how and capability to defend themselves against cyberattacks. To this end, the government will focus its resources, coupled with those of the industry, on developing and implementing the Active Cyber Defense approach (see below) that will minimize the cyberattacks under normal circumstances, including phishing attacks, filtering of malicious IP addresses, and active blocking of malicious activity.[14] The state's capability to thwart these basic types of attack will improve the British defense capability against most of the known cyber threats.

**Deterrence**: The aim is to fortify the British cyberspace against all forms of aggression, while identifying, understanding, investigating, and thwarting attack attempts. In addition, this involves chasing attackers and prosecuting them, including offensive activity in cyberspace. Britain will convey clear messages to its enemies about the expected outcomes of any threat or attempt to harm its interests or those of its allies in cyberspace.

**Development**: This is designed to support innovation and the growth of the British cyber industry. Inter alia, at stake is scientific research and development; investing in human resources in the public and private sectors; investing in the training of analysts and experts in relation to future cyber threats; investing in research with a long-range perspective, with the aim of encouraging the development of human capital comprised of academic scholars in the field of cyber.

**International activity**: Designed to deepen the current cooperative efforts with Britain's neighboring international partners and create new cooperative efforts to build capabilities that will help to secure UK assets throughout the world. These types of cooperation will be achieved through bilateral and multilateral agreements that will include the European Union, NATO, and the UN.

14 According to the government data, a total of 54,456 cyberattacks have been thwarted since June 2016 (phishing and infecting websites with viruses). About 36 percent of these attacks originate from British IP addresses. 64 percent targeted government websites specifically in order to obtain citizens' personal details from government databases.

The joint report of the National Crime Agency and the National Center for Cyber Security (NCSC), which was published in March 2017, stresses the need for cooperation between industry, government, and law-enforcement agencies in Britain, given the intensifying cyber threat and the rapid changes in this arena. The report focuses on the process whereby criminal elements are learning about how state players attack organizations like financial institutions; the risk of the Internet of Things, given the rise of the number of connected devices, most of which are not secured, neither by the manufacturers nor by the users; and the rise in the number of DoS attacks, accompanied by extortion and ransom demands.[15]

## Implementation of the British National Strategy in Cyberspace

In order to achieve the objectives defined in the National Cyber Strategy for 2016–2021, in 2016, the British government decided to invest GBP 1.9 billion in cybersecurity. This decision was reached after a series of strategic cyberattacks on political institutions, political parties, and parliamentary bodies, and the collection of information about British national infrastructure. As an initial step towards improving cybersecurity, the British cyber system was reorganized and the NCSC was established,[16] which was given national operative responsibility over the entire field of defending the cybersecurity in Britain. This responsibility includes, inter alia, knowledge sharing, contending with vulnerabilities, and professional leadership of cybersecurity at the national level. Since the British security system possesses strong capabilities in protecting its internal systems and is required to conduct flexible independent operations, it was decided that the NCSC will cooperate with the military's Cyber Security Operations Center and create an interorganizational platform that will enable the British military to take part in the defense against cyber events that could potentially cause strategic damage at a national scale.

The NCSC was officially launched in October 2016 as part of the GCHQ. The vision behind its establishment was to create a headquarters that would

15 "The Cyber Threats to UK Businesses, 2016/2017 Report," *NCSC & NCA*, March 14, 2017 http://www.nationalcrimeagency.gov.uk/publications/785-the-cyber-threat-to-uk-business/file.

16 "The Launch of the National Cyber Security Center," *National Cyber Security Center*, February 13, 2017, https://www.ncsc.gov.uk/news/launch-national-cyber-security-centre.

manage cyberattacks during emergencies; provide guidance on a routine basis and during states of emergency; serve as a knowledge center for the British cyber community; and constitute the liaison between government and industry. The NCSC became an ecosystem for existing cybersecurity bodies, including the Center for Cyber Assessment, the national CERT, and the GCHQ's Communications-Electronics Security Group, which engaged in information security. Additionally, the new NCSC was delegated the responsibility for all cyber issues that had formerly been under the responsibility of the Center for the Protection of National Infrastructure.

## The Defense Perception

The British cyber defense approach is based on the need to devise a state solution for strengthening defense at a national scale and on instructing the industry to formulate security measures for critical national infrastructure in such vital sectors as energy and transportation. The British defense approach is to be realized through cooperation with industry,[17] including outsourcing, with the aim of using autonomous defense techniques to minimize the impact of cyberattacks being committed by hackers and to catch viruses and spam mail before they reach their intended victims. One of the success indicators as defined by the government in this context is the timeframe during which a malicious website distributing malware remains active. In the past, the duration was about one month, compared to only about two days currently. Another indicator is the number of phishing attack websites registered in Britain that have been removed from the web after about one hour, whereas in the past, it took about twenty-four hours until they were removed.

The British defense approach also prescribes that a large portion of the government's investments in cybersecurity be allocated to strengthen the cyber capabilities of the law-enforcement agencies and to create a defense response that would substantially increase the cost of cybercrimes, in addition to forming international cooperative efforts and building offensive cyber capabilities as a response to state attacks against Britain. As part of the

17 An example of cooperation with the cyber industry is by encouraging the national CERT to form cybersecurity clusters to share and expand the knowledge about cyber defense topics. These clusters are dispersed throughout Britain and operate on an independent, voluntary and informal basis. For the list of clusters, see: https://www.ukcybersecurityforum.com/cyber-security-clusters. HM Government, *National Cyber Security Strategy 2016–2021*, p. 33.

strengthening in these areas, more than fifty cyber researchers and technology experts were recruited for the national cybercrime unit and dozens of millions of GBP were allocated to fight cybercrime.

## Active Cyber Defense

In order to implement the security measures needed at the national level, an approach was formulated called Active Cyber Defense (ACD).[18] In the commercial context, the term ACD usually relates to analyses of cybersecurity risks, developing an understanding of the threats on the web, and implementing pro-active measures that are needed as a defense response. In its British National Cyber Strategy, the government opted to implement the commercial approach in a broader context: it will reflect its unique capabilities in order to influence the measures to be taken against the spectrum of cyber threats. According to this approach, "the web" represents the entire British cyberspace at the macro level. To achieve this target and reduce the cyber threats against Britain—including those by organized crime cartels and state entities with malicious intentions—the authority and capabilities of the GCHQ, the Department of Defense, and the National Crime Agency will be expanded.

The success of the ACD approach will be measured according to the following outcomes:[19]

- The establishment of a broad defense system that will hinder attempts at phishing, SMS spoofing, and spoofing attacks as part of social engineering campaigns
- Blocking of malware
- Protecting traffic on the internet and communications networks against rerouting attempts
- Enhancing the capabilities of the GCHQ, the National Crime Agency, and the British military in providing an effective defense response to strategic cyberattacks

## Knowledge Sharing

One of the key insights of the British cyber strategy is that most of the attacks are committed using basic attack tools, and correct preparedness by organizations could prevent them. To this end, the GCHQ created a platform

18 Ibid., p. 33.

19 Ibid., p. 35.

for knowledge sharing and wrote a user manual called "Cyber Essentials," which is useful mainly for defending small and medium-sized businesses.[20] The National Cyber Security Center also wrote a user manual addressing cyber risk assessment called "Ten Steps to Cyber Security."[21] These courses of action also have regulatory implications pertaining to the definition of the standard by which British organizations should prepare themselves in terms of cyber threats.[22]

Another authority involved in cybersecurity in Britain is the Office of Cyber Security and Information Assurance (OCSIA). Operating at the government level, its roles are to support the cabinet ministries and the National Security Council in relation to all aspects of cyber by offering strategic guidance and coordinating the cybersecurity plans at the government level.[23] OCSIA works in cooperation with government ministries and government agencies, such as the Office of Homeland Security, the Ministry of Defense, the Ministry of Foreign Affairs, the Ministry of Communications, and the GCHQ. OCSIA is also in charge of allocating resources and coordinating between the government ministries on cyber-related issues. It also engages in aspects of cyber policy that interface with the private sector. In the future are plans to establish a body called the Emerging Technology and Innovation Analysis Cell (ETIAC). ETIAC will be tasked with identifying technological developments, threats, and opportunities for national security and government cyber bodies.[24]

Another body tasked with state responsibility on topics relating to cybercrime is the National Cyber Crime Unit (NCCU).[25] The NCCU, which is subordinate to the National Crime Agency, began operating in

20 HM Government, "Cyber Essentials," http://www.cyberaware.gov.uk/cyberessentials/.

21 National Cyber Security Center, "10 Steps to Cyber Security," April 10, 2016, https://www.ncsc.gov.uk/guidance/10-steps-cyber-security.

22 "Minister for Digital and Culture Matt Hancock's speech at the Cyber Security Institute of Directors Conference in London," March 27, 2017, https://www.gov.uk/government/speeches/matt-hancocks-cyber-security-speech-at-the-institute-of-directors-conference.

23 See the OCSIA website: https://www.gov.uk/government/groups/office-of-cyber-security-and-information-assurance.

24 It should be noted that a consulting team for strategic thinking, the Secretary's Advisory Group on Horizon Scanning (CSAG), operates in the cabinet.

25 See details about the agency: http://www.nationalcrimeagency.gov.uk/about-us/what-we-do/national-cyber-crime-unit.

2013 and leads and coordinates the state response to cybercrimes, including the provision of support to its partners in the security system. The NCCU operates in cooperation with Regional Organized Crime Units, the London Metropolitan Police Cyber-Crime Unit, industrial entities, government bodies, and international law-enforcement units.

The Cyber-Security Information-Sharing Partnership began operating in Britain in 2013. This platform encompasses more than two thousand public organizations and private companies. The British companies and organizations also have access to IBM's X-Force Initiative, which provides more than 700 terabytes of information about cyber threats.[26]

## Research and Development

The encouragement of R&D is reflected in the decision to establish cyber innovation centers that advance cyber solutions and constitute infrastructure for the establishment of new cyber companies as well as a foundation to fund cyber innovation, with the support of start-up companies and academic research studies in collaboration with industry. In total, approximately GBP 165 million were allocated within the framework of the 2016 Cyber Strategy to support innovation in the fields of cyber defense and security.[27]

In addition, Britain established the Cyber Security Research Institute that brings together the country's leading universities to engage in strengthening the security of smart devices. The NCSC and the GCHQ support innovation and research on cyber topics for school-age children. One of the programs that the GCHQ funds is the Cyber First Program, with some 2,500 pupils between the ages of 11 and 17 taking part in free cyber courses.[28] The program also includes a cyber competition for girls between the ages of 13 and 15.[29]

Approximately 250 students studying relevant professions in academic frameworks receive annual scholarships valued at GBP 4,000 per annum, with the aim of reaching a total of one thousand students by 2020. The NCSC

26 Royal Society, *Progress and Research in Cybersecurity*, p. 42.

27 Ibid., p. 10.

28 "Applications open for GCHQ's Cyber Summer Schools," *GCHQ*, May 20, 2016, https://www.gchq.gov.uk/press-release/applications-open-gchqs-cyber-summer-schools.

29 "National Challenge will Develop Schoolgirls' Cyber Security Skills," *GCHQ,* January 18, 2017, https://www.gchq.gov.uk/press-release/national-challenge-will-develop-schoolgirls-cyber-security-skills.

and the GCHQ cooperate with about twenty leading universities throughout Britain in offering twenty courses to master's degree students, whereby the students carry on for an additional year of advanced integrative studies in digital forensics, computer science, and cyber studies. The NCSC also launched several research initiatives, which include a plan for establishing thirteen academic centers of excellence in cybersecurity research and awarding scholarships to thirty PhD students who were selected from the centers of excellence. The NCSC also established the government's Cyber Security Innovation Center, which serves as an incubator for start-up companies.

In 2017, the GCHQ published an RFP for the funding of initiatives and research, and established an accelerator for cyber-related start-up companies.[30] This accelerator program includes, at the initial stage, seven start-up companies that receive support from such corporations as Telefónica and Cisco. The GCHQ's intention is to find start-up companies, such as Cyber Owl, which developed an early-warning system that provides intelligence in real time; Status Today, which developed an artificial-intelligence platform to analyze human behavior in the workplace and prevent attacks from within the organization; and Elemendar, an artificial-intelligence platform for analyzing risk reports.

Another initiative that focuses on government and industry cooperation in funding cyber research studies in academia is the Cyber Invest Program. The British government announced the program in 2015, as part of the cooperation with local industry, with the intent of implementing cyber research studies at the commercial level. This program is part of the GBP 165 million allocated for cyber defense and innovation, with the objective of helping start-up companies reach commercial achievements and helping noncommercial cyber initiatives.[31] In the year following the announcement of the program, eighteen companies undertook to invest GBP 6.5 million in this field over the next five years.

Another cybersecurity research body was established in 2013, the Research Institute in Science of Cyber Security (RISCS).[32] Its purpose is scientific

30 "The first-ever GCHQ-backed Accelerator Programme for Cyber Security Start-ups Concludes Today, with all Parties Involved Hailing it as a Huge Success," *Wayra,* March 30, 2017, https://wayra.co.uk/first-cyber-security-start-ups-graduate-from-unique-gchq-cyber-accelerator-programme/.

31 Royal Society, *Progress and Research in Cybersecurity*, p. 60.

32 See the institute's website: http://www.riscs.org.uk.

development and the creation of standards and action methodologies for decision-makers in the field of cyber. RISCS is funded by the GCHQ and the Engineering and Physical Sciences Research Council.

## International Activities

In 2016, Britain funded programs to strengthen the national cyber strength and to support thirty-five projects in about seventy countries worldwide, at the cost of GBP 3.5 million. One of the countries where Britain has joint cyber research programs is Singapore. The joint cybersecurity R&D program between the two countries was launched in 2015, and it includes funding research studies in this field.[33] Since the program was launched, six joint research programs have been operated, at an estimated cost of GBP 2.4 million.[34]

Britain has signed cyber cooperation agreements with the United States, Australia, New Zealand and Canada.[35] Britain's international cooperation in the field of cybercrime is under the responsibility of the National Crime Agency, which maintains connections with Interpol, Europol, and additional agencies.[36] In recent years, British governments have also been promoting strategic cyber-related dialogues with various countries. In 2016, Britain formulated a policy communique with China to deepen the cyber efforts between the two countries, including the design of an intelligence-sharing mechanism, cooperation during states of emergency, and more.[37] During that

33 See the program's website: https://www.nrf.gov.sg/funding-grants/international-grant-calls/joint-singapore-uk-research-in-cyber-security.

34 Ankit Panda and Conrad Prince, "On the United Kingdom's Cyber Strategy and Asia," *The Diplomat*, October 15, 2016, http://thediplomat.com/2016/10/conrad-prince-on-the-united-kingdoms-cyber-strategy-and-asia/.

35 "What is the Five Eyes Intelligence Alliance?," *France 24*, March 17, 2017, http://www.france24.com/en/20170317-what-five-eyes-intelligence-alliance.

36 "International Cooperation," *The National Crime Agency*, http://www.nationalcrimeagency.gov.uk/about-us/working-in-partnership/international-cooperation.

37 Cabinet Office and Foreign & Commonwealth Office, "China-UK High-Level Security Dialogue: Communique," policy paper, June 13, 2016, https://www.gov.uk/government/publications/china-uk-high-level-security-dialogue-official-statement/china-uk-high-level-security-dialogue-communique.

same year, the governments of Britain and India published a joint statement about strategic cooperation between them, including in the field of cyber.[38]

## Shortcomings in the Implementation of the British Strategy

Despite the substantial increase of the British budget for defending cyberspace for the years 2016–2021 and the reorganization and pooling of the powers of the cyber defense arms in Britain, many challenges and deficiencies still hamper the assimilation and effective implementation of the British cyber strategy. The British government's policy of actively influencing the processes of developing technological innovation in the field of cyber defense requires the creation of balances between the security, technological, economic, and social components. Nonetheless, the security component appears more dominant than the other components and serves as a central axis through which the government operates to create conditions that will enable the development of knowledge and an innovative technological environment. From the defense-security perspective, and particularly given the historic structure of the British security and enforcement system, it is only natural that the GCHQ divisions will coordinate the high-level defense capability. This axis, however, constitutes a disadvantage in all that pertains to the interfaces maintained outside of the British security system, which can assist in the synergies between the security system and the civilian system, such as developing academic knowledge, training high-caliber professionals, reciprocities between industry and academia, business development, and technological innovation. The GCHQ's dominance also impedes Britain in all matters pertaining to cooperation with global technology companies. In other words, the decision of the designers of the British strategic approach to base it on Britain's existing resources for defending against cyber threats creates a built-in failure, which poses challenges to implementing the desired response. This failure is reflected, inter alia, in the lack of significant encouragement provided to global technology companies for promoting development, research, and significant business efforts in Britain.

38 Prime Minister's Office, "Joint Statement between the Governments of the UK and India," press release, November 7, 2016, https://www.gov.uk/government/news/joint-statement-between-the-governments-of-the-uk-and-india.

In addition, there are those who point to a similarity between the structure and policy of the British cyber system and those of the State of Israel. This comparison has not withstood the test results as it pertains to the difficulties of the British model in enabling an efficient ecosystem encompassing security, industry, education, and academia. For example, Israel maintains a high level of competition in the global cyber market, due to its graduates of technology units in its security system who have established successful companies that provide dual security products designed for both security and civilian use, and/or security technologies for which civilian applications can be found. The relative advantage of the Israeli security system is that it does not necessarily invent the technology but rather adjusts it to civilian developments in the private market according to its needs. On the other hand, the situation in Britain looks different and, in many instances, is even the opposite: the British security system contributes its share to technological development, but only a portion thereof is transferred to the civilian market. Consequently, the British governmental mechanism constrains the local cyber industry's ability to maintain a relative advantage in the reality of global competition and relative to emerging threats. This situation will remain as long as the British government continues to invest most of its cyber defense budget in the agencies charged with this task. One can assume that many resources in the government's cyber defense budget that are allocated to the British security and intelligence agencies, such as the GCHQ, are still being allocated to offensive and not defensive capabilities, and more resources are allocated to defending critical infrastructure than to defending other infrastructure. To close this gap, Britain needs to consider severing the NCSC from the GCHQ, either fully or partially, and turn it into more of a civilian body to which the private sector has access. Britain also needs to better and more fully utilize the exchange of technological information and solutions between the British security sector and civilian industry. A correct way to implement this is by taking a holistic approach that will distribute the resources more evenly between security and investments in education, academia, and the private sector.

Finally, Britain's exit from the European Union is expected to have implications on its national cybersecurity. Britain's exit will apparently lead to its departure from EU organizations, such as the European Cybercrime Center and, consequently, it will no longer be a partner in the European Union's

cybercrime prevention efforts. It is not yet clear what Britain's policy will be regarding joint regulatory issues among member states of the European Union, such as the General Data Protection Regulation, and to what extent its policy will change once Britain leaves the European Union.[39] Once it exits the European Union, Britain will have to contend more vigorously with the recruitment of high-caliber manpower for cyber professions. In November 2015, cybersecurity was added to the list of professions that are in short supply in Britain. Consequently, citizens outside of the European Union will be allowed to submit applications for work visas in Britain. Britain's exit from the European Union is liable to lead to the opposite scenario, whereby British cyber professionals will opt to work in other countries (where the income levels and the opportunity of professional mobility will be higher after Brexit). Furthermore, Britain will be forced to find budgetary means to fund academic research in technological fields that today are partially funded from European Union budgets. A short-term solution for this would be to divert resources that were earmarked for research and development and for financing European Union funds in order to open special academic research funds in the British centers of knowledge. On the other hand, Brexit is not expected to adversely affect Britain's strategic cyber partnerships with the "Five Eyes" countries (Australia, Canada, New Zealand, Britain, and the United States).[40]

## Conclusion

Britain made a long-range strategic decision about national cybersecurity, which includes strengthening the national resilience in cyberspace in general and in digital space in particular, through government investments designed to create human capital from the school level, including the establishment of centers of excellence in cyber security research and cyber accelerator programs for start-up companies. Some of the resources are be devoted to reorganizing the cyber defense arrangement and to recruiting cyber experts for Britain's law-enforcement authorities and intelligence agencies. The

39 A resolution within the scope of the GDPR, which is expected to come into effect in the European Union during 2018, requires companies registered in the European Union to notify their governments about cyberattacks against them within 72 hours. See also the European Information Security website: http://www.eugdpr.org.

40 "The Implications of Brexit on UK Cyber Policy," *Council on Foreign Affairs*, June 28, 2016, https://www.cfr.org/blog/implications-brexit-uk-cyber-policy.

jewel in the crown of Britain's strategy is the establishment of the National Cyber Security Center, which is tasked with building a bridge between the government and industry and with providing guidance and management during states of emergency, including cyberattacks targeting critical national infrastructures.

Alongside building offensive deterrence capabilities, Britain is working towards reducing "basic" cyberattacks in the short-term, which constitute most of the attacks against it. Additionally, Britain formulated a vision whereby topics, such as autonomous systems, the Internet of Things, and smartphones—which will constitute most of the medium-range threats—will already receive a response through the establishment of an academic and commercial research infrastructure that will try to contend with the challenges and threats over time.

Britain's National Cyber Security Strategy for 2016–2021, which received a budget of about GBP 1.9 billion, focuses mainly on implementing the approach of self-reliance on the technological and human resources for the purpose of defense, the creation of deterrence mechanisms, and international cooperative efforts. It appears that, unlike in the past, when the GCHQ and the British security organizations relied on their own systems in all matters pertaining to the fields of security R&D, the current British approach encourages decentralization of capabilities and research and also includes a new strategy, whereby the GCHQ is more open than in the past to cooperation with civilian and public bodies in order to promote technological innovation and to develop human capital and the growth of the British civilian cyber market.

Notwithstanding the efforts exerted to date, many challenges and gaps continue to hinder the assimilation of the British cyber strategy. Among the challenges is the excessive concentration of the British cyber defense structure under the GCHQ and Britain's expected exit from the European Union. A possible solution to these challenges is a more balanced distribution of resources between investing in cybersecurity and investing in education, academia, and the private sector.