A HOOVER INSTITUTION ESSAY

Adapting to the Cyber Domain

COMPARING US AND UK INSTITUTIONAL, LEGAL, AND POLICY INNOVATIONS

ROBERT M. CHESNEY

Aegis Series Paper No. 2103

Prime Minister Boris Johnson made it official in a statement to Parliament on November 19, 2020. "I can announce that we have established a National Cyber Force, combining our intelligence agencies and service personnel," he proclaimed, adding that it "is already operating in cyberspace against terrorism, organised crime and hostile state activity."[1]

Public avowal of the National Cyber Force (NCF) came as no great surprise. Plans to take this institutional step had been discussed publicly before, after all.[2] Nonetheless, it was a significant moment in the ongoing process of tailoring UK institutions, policies, and legal frameworks to suit the evolving nature and scale of cyber domain threats and opportunities. The NCF embodies certain distinctive characteristics of the British system, including flexibility regarding institutional roles in general and the role of intelligence agencies in particular. Much the same can be said, moreover, for another recent British organizational innovation: creation of the National Cyber Security Centre (NCSC).

The American experience throughout this same period has been analogous in many respects—including the creation of new organizations with defensive and offensive missions—yet it is by no means identical. As we shall see, institutional formalism is far more conspicuous in the American system, and so too are anxieties about the roles of intelligence agencies. Whether these are bugs or features is, perhaps, in the eye of the beholder. The comparison between the UK and US models, at any rate, is instructive.

In the pages that follow, I explore the origins and evolution of the institutional, policy, and legal frameworks that have come to define both the defensive and offensive aspects of the UK and US models. The first part below focuses on *defensive* functions that all governments pursue, from protecting their own systems to helping with private-sector defense. Both the United Kingdom and the United States have engaged in a variety of institutional and policy innovations over time in an attempt to perform such functions, in both cases culminating recently in the establishment of new organizations that differ in intriguing ways. The second part below focuses on *offensive* functions: that is, government activities that entail overcoming rather than enhancing computer security. Both the US and UK governments have developed such capacities in service of familiar public policy priorities, ranging from the familiar (law enforcement, espionage, and armed conflict) to the exotic (adversarial statecraft below the level of war). Some of the resulting activities fall readily within the

domains of well-established government institutions in both the United States and the United Kingdom, but others present harder questions of institutional design and legal architecture.

COMPARING US AND UK ADAPTATIONS FOR DEFENSIVE FUNCTIONS

All governments engage in a variety of activities to defend both themselves and their societies from unwelcome interventions by other states. From counterintelligence to military defense, these are familiar defensive functions for which governments have long-established institutions, along with legal and policy architectures that both enable and (in some countries more than others) constrain them.

There is nothing novel about the general idea that technological change can unsettle those institutional, policy, and legal arrangements. History is replete with—arguably even defined by—an endless succession of such developments. From steam power to nuclear power, from the rise of aircraft to the submerging of submarines, the practical possibilities relating to how states pursue their national interests in relation to one another are in constant flux. Incumbent structures—especially those involved in national defense and intelligence—have to adapt, sooner or later, both to exploit and to defend against the new possibilities that changes of this kind generate.

In some cases, technological change requires recognition of an entirely new domain of activity. So it was with the power of flight, with the resulting creation of air forces, international civil aviation arrangements, and (mostly unsuccessful) attempts to prevent the emergence of aerial bombing. So too with submarine technology and space-related technologies. And so too, obviously, with the proliferation of computers and networks that combine to constitute the cyber domain.

Predictably, the rapid growth of the cyber domain is having a significant disruptive impact on every nation's institutions and legal architectures. The features of the cyber domain that drive this disruption are well understood. They include the sharply reduced relevance of physical proximity as a constraint on the ability of one state to reach another; the relative difficulty (however often it is exaggerated) of reliably attributing a particular action in the cyber domain to a particular state; the speed with which operations are performed; the astonishing growth of data and systems that can be reached and thus put at risk of theft or even destruction; the relative affordability and practicality of establishing significant government capabilities to operate in this domain; the overlap with a globalized black market for increasingly capable hacking tools and services; the ability of private actors to have impacts akin to those previously thought the province of governments; and so forth.

Taken as a whole, these features result in a world in which more actors are more able to spy on one another, to steal from one another, to hold one another's valued assets at risk, and,

in extremis, to harm one another. Our increasingly wired world is becoming more efficient, but also more dangerous in this sense.

Both the United Kingdom and United States governments are in the midst of a protracted process of adapting to these rapidly evolving circumstances. They have pursued similar paths, but not identical ones. My aim in this first part is to describe their respective evolutions in terms of the *defensive* mission (i.e., protecting the confidentiality, integrity, and availability of information systems and associated data, particularly those systems and data associated with the government and with critical infrastructure).

Evolution of the US Defensive Model

In his book *Dark Territory*, Fred Kaplan opens with a vignette of President Ronald Reagan watching the hacker classic *WarGames* at the White House in 1983. The film features Matthew Broderick as a teenage gamer who thinks he is hacking into a software company's game development system when, in fact, it is a Pentagon system with its proverbial finger on the nuclear button. Reagan was alarmed by the film's depiction of poorly secured military code, and he pressed the Pentagon on whether anything of that sort could happen with real military systems. The answer, alas, was not reassuring.[3]

That was nearly four decades ago. Things have improved a vast amount since then. Perhaps not as much as one might expect, however. And what progress there has been has not been equally distributed across government national-security systems, civilian government systems, and privately held critical infrastructure systems.

Not surprisingly, the path forward turned out to be smoothest with respect to enhancing the security of America's "national security systems" (NSS)—that is, those information systems associated with the US government's military and intelligence activities. Progress in this area has been facilitated by a combination of factors. Critically, the National Security Agency (NSA) was well suited to adapt to this task. And though institutional changes were needed across the broader military establishment, the US Department of Defense (DoD) by its nature has unusual capacity to reorganize itself compared to other government entities. In contrast, there was no comparable incumbent institution arching across the numerous departments, agencies, and offices that constitute the rest of the executive branch. And the obstacles are still more difficult once one turns to the private sector and critical infrastructure.

Cybersecurity for National-Security Systems

As long as there have been military communications worth intercepting and reading, there have been efforts by adversaries to acquire them and, if necessary, decrypt them. The military, accordingly, has a long history of pursuing communications security (COMSEC), particularly via cryptography but also through the screening of hardware—and eventually

of software too. Since the early 1950s, these capabilities have been concentrated in the Defense Department's NSA, an agency far better known for its signals intelligence (SIGINT) espionage and analysis efforts.[4]

By the late 1970s, under the directorship of Admiral Bob Inman, NSA was beginning to expand its information security services more broadly throughout DoD. As Kaplan relates, NSA thus was in a good position to take on a still bigger role when Reagan's 1983 inquiry began to filter through the Pentagon.[5] At the same time, however, the idea of an expanded NSA role was anathema to others (especially to civil liberties advocates still flush with concerns rooted in domestic spying scandals that emerged in the 1970s). Ultimately, NSA assumed the key role in setting security standards for "national security systems," but Congress effectively blocked it from doing the same for the rest of the executive branch.[6] We will return to the topic of security for the rest of the executive branch shortly. For now, it is enough to say that what became NSA's Information Assurance Directorate (since folded into NSA's Cybersecurity Directorate) performs the full spectrum of security functions for national security systems—that is, the systems handling classified information.

There is much more to the military's cybersecurity history than just NSA's role, however. Not every inch of attack surface related to military information technology (IT) is within the NSS domain, and NSA does not operationally defend all of it. Additional security-oriented structures were needed.

That need was documented, famously, by Cliff Stoll's book *The Cuckoo's Egg*, describing the seemingly endless and often comical futility of his efforts in the mid-1980s to alert government and military officials to a security breach involving military systems.[7] Of course, one might expect the situation to have improved a great deal over the decade that followed. Alas, the experience of 1997's Eligible Receiver exercise, during which an NSA "red team" quickly ran rampant through some of DoD's most crucial networks, suggested otherwise. As Kaplan relates, Deputy Secretary of Defense John Hamre was stunned to discover in the aftermath of that exercise how poorly prepared DoD was to address its cybersecurity failings.[8] And when that same lack of responsibility became still more glaring amidst the actual hacking episode known as Solar Sunrise, Hamre pressed for a solution.

He got one, or at least the beginning of one. Brigadier General John "Soup" Campbell of the Joint Chiefs of Staff J-39 bureau proposed formation of what came to be known as Joint Task Force-Computer Network Defense (JTF-CND). On paper, at least, JTF-CND consolidated a variety of defense-oriented operational functions. By late 1998 its skeleton was in place, building on the intrusion-detection and other network-monitoring capabilities developed by the Air Force's Information Warfare Center in San Antonio.[9]

The first major change to JTF-CND involved an expansion of its remit to encompass, at least notionally, computer network *attacks* in addition to its original defense mission,

and a corresponding change to the JTF's name. It remained limited in practice, however, along critical dimensions including the number of expert personnel it could bring to bear, the technical infrastructure (from exploits to staging servers) it could access, let alone develop on its own, and the authorities it possessed to act. All that began to change, however, when Secretary of Defense Robert Gates in 2009 transformed the JTF into US Cyber Command (USCYBERCOM) and intertwined it with NSA for incubation purposes.[10]

The incubation model was a bold stroke. Going forward, at least for a time, USCYBERCOM and NSA would share a single "dual-hatted" commander, ensuring (at least to some degree) an inherent understanding of and interest in the respective capabilities and missions of the two organizations where it would count most for purposes of cooperation on a day-to-day basis. Equally critical, USCYBERCOM would be co-located on site with NSA at Fort Meade and would share personnel and technical infrastructure. It is hard to imagine an approach that would more efficiently produce a rapid surge in USCYBERCOM's capabilities, for both its defensive and offensive missions, while also minimizing the deconfliction problems inherent to the overlapping interests of intelligence agencies and the military in cyberspace.

USCYBERCOM today is a full-fledged combatant command (rather than just a supporting command akin to a service branch) and has matured to the point of triggering a lively debate regarding whether to sever the dual-hat relationship and other elements of the incubation model. For now, however, what matters is that USCYBERCOM hosts a relatively well-developed institutional structure for the larger DoD defensive mission, apart from NSA's role. That mission is concentrated in a subordinate command called Joint Force Headquarters–DoD Information Network (JFHQ-DoDIN).

JFHQ-DoDIN performs several critical defensive functions. First, it is a centralized mechanism for making DoD-wide determinations relating to cybersecurity risk-management policies and practices. Second, it oversees compliance with those policies across the DoDIN. Third, it issues directives when necessary to compel or prohibit particular actions by a given DoD component. Fourth, it provides a degree of centralized operational defensive services for DoD. And fifth, it can deploy personnel (Cyber Protection Teams) to provide further operational defensive services in specific settings if and when needed (that is, where the in-house operational capabilities of personnel defending a particular DoD organization are not sufficient to the task).

Cybersecurity for Federal Civilian Systems

Change has come far more slowly with respect to the vast array of federal government organizations that are not part of the military or the intelligence community and that sometimes are called, collectively, the Federal Civilian Executive Branch (FCEB).

The issue of FCEB cybersecurity began to get sustained attention in the mid-1990s. In 1996, Congress took an important preliminary step by creating a standards-setting function applicable to the FCEB as a whole. Going forward, the secretary of commerce would promulgate cybersecurity standards for all FCEB entities, drawing on the expertise of the National Institute of Standards and Technology (NIST) to do so. Unfortunately, Congress did not also empower Commerce (or any other entity) to audit and compel actual compliance with those standards.

Not long thereafter, Dick Clarke (famous for his efforts during the Clinton and George W. Bush administrations to draw attention to a variety of emerging threats, including cybersecurity and terrorism) proposed a bolder intervention: centralizing most, if not all, FCEB network infrastructure in order to facilitate monitoring of traffic at the network perimeter, possibly to be implemented by NSA. The proposal generated sharp pushback, however. Many still viewed cybersecurity as a prosaic aspect of IT management that should be left to the purview of the specific agencies, and the possible role of NSA added a privacy-protection dimension to the opposition. The proposal crashed and burned.[11]

Congress came back to the drawing board in 2002, enacting the Federal Information Security Management Act (FISMA).[12] FISMA improved the existing standards-setting process in two promising ways. First, it shifted responsibility for promulgating NIST-based standards from Commerce (which had little purchase over other departments) to the White House Office of Management and Budget (OMB) (which had, at least in theory, a great deal of potential leverage). Second, FISMA gave OMB authority to monitor other agencies for actual compliance.

On a separate front, however, FISMA also innovated institutionally by mandating creation of what became US-CERT (Computer Emergency Readiness Team). US-CERT was not there to perform centralized security services à la the Clarke model, but it would be able to provide expert advice throughout the FCEB both ex ante (that is, pre-incident) and in specific response to an incident. This was a modest but significant step toward the possibility of centralized defensive services.

Other waves of innovation followed. By 2008, the Department of Homeland Security (DHS) existed, and it included a component, known then as the National Protection and Programs Directorate (NPPD), with at least nominal responsibilities relating to physical security and cybersecurity for both privately held critical infrastructure and the FCEB. President Bush decided to place US-CERT within NPPD, and then added a fresh element of centralized defensive services: in a variant of Clarke's original plan, Bush directed NPPD to create a threat-detection capability for all FCEB network external access points. This resulted in the creation of a signature-based sensor system that monitors inbound and outbound traffic for indicators of compromise and the like, to be known as "EINSTEIN."[13] Bush also called

for NPPD to develop other defense-oriented services that other parts of the FCEB might choose to use. Then, in 2010, President Barack Obama directed OMB to delegate to NPPD its compliance-checking function (overseeing FCEB compliance with the NIST standards), a move that Congress ratified in a 2014 update to FISMA.

With that 2014 FISMA update, Congress took an important additional step. Up until that point, NPPD had lacked any enforcement authority. It could not impose direct costs on recalcitrant FCEB entities for failing to comply with NIST standards, and it certainly could not issue specific directives to other agencies making them take security measures. FISMA 2014 left the former gap in place, but it closed the latter one by authorizing NPPD to issue "binding operational directives" that compel FCEB entities to take particular actions in response to known or reasonably suspected vulnerabilities and other information-security risks.[14]

NPPD's first use of this authority provides a good illustration of the need for it. NPPD had a program that scanned FCEB systems for known vulnerabilities, and each week would provide relevant departments and agencies with a customized report flagging critical vulnerabilities on their systems, as well as describing the needed mitigation steps. Uptake on that information was not, however, anything like what it should have been. With the authority to issue binding operational directives, however, NPPD could now do more than make recommendations. Its first binding operational directive, in May 2015, gave agencies thirty days to act on critical vulnerability notifications impacting their internet-facing systems, or else provide a detailed account explaining the basis for any delay and the plan for eventually making the required changes. Congress supplemented the binding operational directive authority the very next year, moreover, adding a somewhat-overlapping capacity to issue Emergency Directives to compel action by the head of an FCEB agency in response to information-security threats.

The next stage in this evolutionary process was of a different order: rebranding the anodyne-sounding NPPD as the Cybersecurity and Infrastructure Security Agency (CISA). This shift might seem inconsequential in formal terms, but perceptions matter, and branding can impact perception. The mission-specific clarity of the CISA brand helped spread understanding of the maturing organization's role both within the FCEB and, as we shall see, with the private sector as well. The timing in late 2018 was impeccable, moreover, given the degree to which the organization's authorities had matured by that stage and the fact that it enjoyed a particularly effective leader in the person of Chris Krebs.

Over the next two years, CISA polished and expanded the defensive services it could offer to the FCEB as well as to state and local government entities and to privately held critical-infrastructure entities. The list encompasses everything from threat hunting and incident response (remote or on-site) to continuous diagnostics and vulnerability scanning.[15] But two key constraints remained. First, CISA was not funded to the degree

needed to provide such services on a comprehensive basis. Second, the entire system until very recently was entirely voluntary, in the sense that CISA could provide its help to an FCEB entity only with that entity's consent. Threat hunting, for example, occurred only upon request.

This is changing at the time of this writing. When Congress in December 2020 overrode President Donald Trump's veto of the National Defense Authorization Act for Fiscal Year 2021, it enacted a raft of new cybersecurity provisions. Among the least noticed but most important of them was Section 1705, which gives CISA express authority to conduct threat-hunting operations on the information systems of FCEB agencies "with or without advance notice to or authorization from" them.[16] The federal government is not yet fully centralized when it comes to defensive services across the FCEB, or even close to being so. But between CISA's authority to conduct threat hunting at will and to issue Binding Operational Directives and Emergency Directives, Congress has moved the government onto firmer ground in recent years. Given the furor surrounding the SolarWinds breach (some of the harm from which might have been avoided had more-effective network monitoring been in place), this change appears to be arriving none too soon. All that authority will be for naught, of course, if it is not matched with the budgetary and personnel resources to execute them effectively and at scale.

Cybersecurity for Private Critical Infrastructure

In the mid-1990s, the security of privately held critical infrastructure (CI) became a subject of increasing federal government interest as concerns about terrorism grew, particularly following the bombing of the Murrah Building in Oklahoma City in 1995. Soon after that attack, President Bill Clinton ordered a committee to develop recommendations on this issue. The resulting Critical Infrastructure Working Group (CIWG), led by Deputy Attorney General Jamie Gorelick, included several participants who were well aware of the cybersecurity vulnerabilities of critical infrastructure, and CIWG became a vehicle for drawing attention to that risk and recommending interventions. This spurred a congressional committee hearing in the summer of 1996, one that identified a litany of obstacles to more-effective cybersecurity in the CI area: the reluctance of private-sector entities to take steps that might erode competitive advantage over rivals; attribution uncertainty that confounded efforts to determine which federal agency should be in the lead in response to an attack (particularly in light of uncertainty as to whether an attack is coming from a domestic or foreign source); "documented distrust of government involvement in this area"; a private-sector preference to seek help from private cybersecurity firms whose main charge was simply to disrupt or stop an attack but not to ensure identification and accountability for the attacker; lack of data to enable reliable threat estimates; lack of expertise and technical capacity among potentially responsible government agencies; and so forth.[17] It also spurred the Clinton administration to create a commission formally tasked with developing solutions.

The resulting President's Commission on Critical Infrastructure Protection (better known as the Marsh Commission, for its chair Robert Marsh) produced a 1997 report (the Marsh Report) that documented the threat in persuasive detail while offering an array of recommendations. The general thrust was to call for a public-private partnership to make progress on CI cybersecurity, centered around the voluntary exchange of information. The voluntary model, the report argued, would "be more effective and efficient than legislation or regulation."[18]

In 1998, these recommendations bore important fruit in the form of President Clinton's Presidential Decision Directive 63 (PDD-63).[19] The directive embraced both the importance of information sharing and the model of relying on voluntary partnerships (both public-private and private-private) to generate improvements to CI cybersecurity. On the organizational side, it called for creation of a National Infrastructure Protection Plan, establishment of a White House "coordinator" position within the National Security Council, identification of lead agencies for each CI sector, identification of specific officials to act as lead liaison officers with private entities in each such sector, and identification of private-sector liaisons to be their counterparts. And this did lead to pockets of success, particularly in the gradual accumulation of sector-specific Information Sharing and Analysis Centers (ISACs)—privately managed voluntary organizations facilitating enhanced sharing of threat indicators and other useful information. Consistent with the Marsh Report, however, there was no talk of regulatory or legislative intervention to impose cybersecurity-related rules on the private sector, let alone direct government access to private-sector systems for oversight or operational purposes.[20]

When President Bush promulgated the *National Strategy to Secure Cyberspace* in 2003, the overall approach remained focused on voluntary public-private partnerships, information sharing, and improved organizational structures to make all of this more efficient. From an organizational-innovation perspective, its most notable feature was to designate the newly created Department of Homeland Security as the notional "single point-of-contact for the federal government's interaction with industry and other partners."[21] As with the contemporaneous decision to insert DHS into the FCEB cybersecurity ecosystem, however, this charge was not yet paired with resources and compulsory authorities necessary to the scale of the task.

In the early years of the Obama administration, the federal approach to cybersecurity for private-sector critical infrastructure stayed relatively constant. That changed to some extent in early 2013, however, with the simultaneous promulgation of Executive Order 13636 and Presidential Policy Directive 21 (PPD-21).[22] Together, these directives sought to boost CI cybersecurity by further encouraging voluntary sharing of information, by directing NIST to develop a risk-management framework (to be known as the "cybersecurity framework"), and by helping CI owner/operators to understand "industry best practices" with respect to "standards, methodologies, procedures, and processes."[23] Notably, Section 9 of the order

called on DHS to identify especially sensitive CI entities (ones where a cybersecurity failure "could reasonably result in catastrophic regional or national effects"), and Section 10 in turn directed relevant regulatory agencies to bear these designations in mind in the course of determining whether new cybersecurity-relevant regulations might be needed.[24]

In the final analysis, however, nothing in EO 13636 or PPD-21 attempted to compel private-sector CI owner/operators to take any particular actions. The president could not simply order the private sector around in that way, after all; that would require legislation.

Toward that end, the Obama administration explored the possibility of including some form of mandatory cybersecurity standards for key private-sector entities, in connection with the legislative process that ultimately culminated in the Cybersecurity Information Sharing Act of 2015.[25] The proposal went nowhere, however. In the end, even the information-sharing provision in the 2015 statute was wholly voluntary from the private-sector perspective, and nothing in it spoke to the question of minimum security standards.

Not long after the act's passage, the administration in 2016 announced a further enhancement of its efforts to promote cybersecurity across several dimensions, including with respect to CI.[26] Among other things, this meant creation of a mechanism whereby CI owner/operators could simulate attacks on their systems and an expansion of DHS personnel charged with assisting private-sector cybersecurity efforts with on-site assessments and support for improvements. These measures contributed to the ongoing maturation of DHS, a trend that continued to accelerate with the transformation of NPPD into CISA (as noted above). Today, CISA is able to offer to the private-sector owners of CI most of the same cybersecurity assessment and support services that it can provide to FCEB agencies (though significant resource constraints limit the practical impact of this capability).

Not surprisingly, no one has yet made a serious effort to confer on CISA (let alone NSA) the ability to provide such services to the private sector involuntarily. Nor, for the most part, is there serious momentum toward a more heavy-handed approach to regulation in this area. The last notable gesture in that direction occurred in 2017 when the Trump administration issued Executive Order 13800.[27] Among other things, EO 13800 directed a review of existing regulatory authorities relevant to cybersecurity for the CI entities deemed most important under the Section 9 framework mentioned above, with a specific charge to identify existing regulatory authority that might be useful to improve security for such entities. It is not clear what effect this review may have had, however.

There is one exception to this general state of affairs involving the Defense Industrial Base (DIB). In 2020, the Department of Defense employed the leverage inherent in its contracting in order to introduce significant new incentives for DIB companies to improve their own cybersecurity and in turn to force their supply chains to do the same.

The DIB acquisitions rules already had nominal requirements of this kind, but with little teeth in terms of a likelihood of auditing for compliance. Now, under the Cybersecurity Maturity Model Certification (CMMC) system, firms would not be able to obtain contracts in the first place without meeting cybersecurity requirements appropriate to the scale and sophistication of their operations and obtaining a certification of compliance from an outside auditor. The actual rollout of CMMC will, inevitably, be a rocky one. If it is successful over time, however, it is not hard to imagine that it becomes a model toward which the US government might turn if and when some shock to the system creates the political will to intervene aggressively to improve CI cybersecurity in general.

Evolution of the UK Defensive Model

In some respects, the UK defensive model closely tracks that of the United States. Like America's NSA, the UK's Government Communications Headquarters (GCHQ) is both a world-class SIGINT-collection organization and an equally capable information-assurance organization. And, like NSA, GCHQ therefore has always played the leading role in protecting the British equivalent to what the US calls national security systems. But whereas the United States rather sharply confines NSA's role, most notably by excluding it from operational involvement in the protection of "civilian" government systems and private-sector systems, the British take a far more flexible approach with GCHQ.

This appears to stem from certain fundamental differences between the United States and the United Kingdom. First, public anxieties about the role of NSA in the United States are considerably sharper than corresponding fears about the role of GCHQ in the United Kingdom. As a consequence, it is simply more toxic, politically, to permit a broad role for NSA, no matter how capable NSA may be. Second, the American legal framework is considerably more formalistic than the UK framework when it comes to the affirmative "authorities" allocated to particular agencies. In the American system, agencies typically conceive of their functional lanes as affirmatively defined and hence bounded; and, more to the point, agencies perceive one another as operating within such boundaries, and will act to protect turf accordingly. The British system, in contrast, operates against a background assumption that general authority to act is there, subject of course to whatever constraints law may impose. In combination, these conditions go far to explain why the role of GCHQ over time has broadened considerably beyond that of NSA, occupying functions that in the US system ultimately required the creation of separate institutions.

The pages that follow trace this evolution and the many nuances and complexities that have arisen along the way. In contrast to the section above on the US defensive model, defined by its distinct subsections on national-security systems, civilian government systems, and private critical infrastructure, here I follow a single, blended chronology—as befits a model that in many ways eschews such distinctions.

Critical National Infrastructure Concerns in the 1990s

In his history of GCHQ, Richard Aldrich describes the arrival in the 1990s of the "new age of ubiquitous computing" and the complicated impact this had on GCHQ. Computing itself had long been central to GCHQ's work, of course, going back to the legendary wartime work of Alan Turing and others at Bletchley Park.[28] As Aldrich points out, however, the driving force behind GCHQ's computing during the Cold War had been the imperative of breaking the encryption used by the Soviets and others, and, by extension, protecting the United Kingdom's own information system from similar efforts by hostile intelligence agencies. The possibility that significant national interests—let alone strategic ones—might become intertwined with the security of run-of-the-mill computer systems and networks, and that GCHQ might play a key role in supporting such security, was not self-evident early on.[29] A gradual shift in priorities was bound to occur, though, thanks to the massive shift toward computer-based communications, commerce, and control of machinery and other tangible systems.

As noted earlier, critical-infrastructure vulnerability drove such a shift in perspective in the United States in the 1990s. So too, contemporaneously, in the United Kingdom, which uses the phrase "critical national infrastructure," or CNI. Aldrich relates a particularly telling incident that unfolded in 1995, in which a number of financial institutions in London were blackmailed by hackers who made a convincing case that they had access to the banks' systems and were in a position to destroy data. The Bank of England and the Department of Trade and Industry were the regulatory leads for this CNI sector. They lacked the expertise to contribute effectively to the cybersecurity aspects of the situation, however. GCHQ, accordingly, was brought in to investigate. This was an early demonstration of the flexibility of the British model in terms of taking advantage of the forensic expertise of the intelligence community in a context involving the private sector. And soon, GCHQ was "under pressure to defend the whole underlying electronic system upon which banking, commerce and indeed all the public services that supported national life now depended."[30] Indeed, GCHQ soon found itself in the awkward position of supporting the use by private entities of advanced forms of encryption, notwithstanding a long tradition (stemming from its SIGINT-collection mission) of resisting the spread of high-grade cryptography.[31]

In the United Kingdom, growing appreciation in the late 1990s for the threat to CNI associated with cybersecurity had the same effect that it was having at that moment in the United States: it led officials to ponder how best to increase the sharing of threat information, and also how to spread awareness of risk-management best practices. As noted earlier, the main US response at that time was to encourage formation of private-sector ISACs. The United Kingdom did this too, in the form of "information exchanges," but it also went a step further by forming a new government entity charged with supporting these information-sharing missions (something the United States would not do until DHS took

on aspects of this mission in the post-9/11 period, and which would take years thereafter to come into its own).[32] Specifically, in 1999, the government formed an interdepartmental organization called the National Infrastructure Security Co-ordination Centre (NISCC). NISCC had no operational role, but rather focused on providing "regularly updated advice and warnings" helping entities engage in "effective risk management and assurance of their systems."[33] NISCC drew on capabilities across the government, most notably including the component of GCHQ that focused initially on information assurance for the UK's "defence and security assets" and, later, for other government entities: the Communications-Electronics Security Group, or CESG.[34]

In this way too, then, the emerging UK model proved open to direct involvement from GCHQ in a way that contrasted sharply with the American model. NSA, after all, plays no direct role in the mechanisms the United States eventually adopted to perform comparable information-sharing and risk-management advice functions for critical-infrastructure owners and operators.

In 2007, NISCC was folded into a new entity focused on CNI protection, the Centre for the Protection of National Infrastructure (CPNI). At that point, it became housed at MI5, the UK's domestic security intelligence organization. As before, however, it had no operational role, but rather focused on sharing advice and other defense-relevant information.[35]

Reorganizing with the 2009 and 2011 Strategies

By 2007, some senior officials were convinced that more ambitious and organized efforts were needed, and that a larger national-strategy framework would be necessary to drive such changes. The government had engaged in a modicum of national strategic planning relating to cybersecurity previously, via the Cabinet Office's periodic publication of "National Information Assurance Strategies" (once in 2003, and again in 2007). These documents made general promises about enhanced government efforts to treat information assurance as a priority, and they broadly encouraged the private sector to have clearer and more-effective risk-management policies. But labels aside, that is a far cry from having an actual national strategy in the sense of setting strategic priorities and matching them with funded initiatives.

In 2007, Prime Minister Gordon Brown commissioned an effort to close that gap. The result that emerged two years later was the United Kingdom's first true cybersecurity strategy document, the "2009 strategy."[36] It endorsed several distinct interventions. Some focused on budgetary commitments. For example, it called for a substantial increase in government funding for development of cybersecurity-related technologies, and likewise for a resource surge intended to expand the pool of people with cybersecurity-relevant training. But it also proposed two important organizational reforms.

First, the 2009 strategy called for creation of an interdepartmental Cyber Security Operations Centre, to be hosted by GCHQ's CESG. The Operations Centre was charged with several missions. One was an intelligence-coordination function (improving the government's collective understanding of the cyber threat environment). Another involved the sharing of threat intelligence and advice for the benefit of the general public, thus expanding on the information-sharing work already performed for CNI owner/operators by CPNI (the former NISCC). The Operations Centre also would have an operational role—helping to coordinate incident response in at least some scenarios. This was something GCHQ already had been doing to some extent, notably, tracing back at least to the 1995 extortion attempts targeting financial institutions in London. And it was another illustration of the way that the British model all along has operated without the same formalistic constraints that define the American model.[37]

A second organizational reform dictated by the 2009 strategy concerned the Cabinet Office itself. Heretofore, attention to cybersecurity matters at that level had been an ad hoc affair, with no sustained commitment and no formal touch points of responsibility. In such circumstances, interdepartmental coordination was more difficult than it might otherwise be. The 2009 strategy sought to change that, identifying seventeen separate "workstreams" relating to the broad goals set forth in the document, and calling for the creation in the Cabinet Office of a new Office of Cyber Security, renamed soon thereafter as the Office of Cyber Security and Information Assurance (OCSIA), charged with monitoring progress across all relevant agencies with respect to the execution of those workstreams.[38]

With Prime Minister Gordon Brown replaced by David Cameron in 2010, and with growing national attention to cybersecurity challenges, it perhaps is not surprising that the 2009 strategy was superseded in 2011 by a new document: "The UK Cyber Security Strategy: Protecting and Promoting the UK in a Digital World" (the "2011 strategy").[39] The 2011 strategy was largely consistent with its predecessor, albeit with still-more-emphatic rhetoric about the nature of the threat and the imperative need to address it effectively. Critically, it also came with a commitment to spend approximately £860 million over a five-year period culminating in 2016: the National Cyber Security Programme.

Sailing before these winds, information-sharing efforts evolved further. In 2013, GCHQ teamed with MI5 and the National Crime Agency to create a single government entity to participate in what would be called the Cyber Security Information Sharing Partnership (CiSP). CiSP expanded on the less-centralized ISAC models already in existence. It is a public-private partnership for the real-time exchange of cyber-threat intelligence, overarching across sectors rather than being specific to a particular one. By 2015, nearly eight hundred private-sector organizations and more than two thousand individuals were participating in its digital-collaboration environment, and it has grown significantly more since then.[40]

Separately, this period also saw the government beginning to play a more proactive role, pushing private-sector entities to adopt specific defensive measures. Specifically, GCHQ began to work directly with UK telecommunications companies to urge them—and to help them—to adopt systems for automated detection of known indicators of compromise (IOCs).[41] However commonplace such in-network threat-hunting methods may be today, they were comparatively novel then in some circles and stood in contrast to more-passive approaches to defense. Perhaps for that reason, the phrase "active defense" eventually became common in UK cybersecurity policy circles as a shorthand for more-active forms of in-network defensive capabilities.[42]

Other institutional innovation followed in that same period. The most visible of these was the establishment of the Computer Emergency Response Team-UK (CERT-UK).[43] The creation of a national-level CERT—something the United States had done long ago and that had caught on as a useful model adopted by many others—was a long time coming for the United Kingdom, and had been a key plank in the 2011 strategy. It addressed a question spawned by the proliferation of cybersecurity entities in recent years: who should be the main point of contact and lead coordinator in the event of a major cyber incident? Given that role for CERT-UK, moreover, it made sense to fold CiSP into that organization. Meanwhile, in 2013, the United Kingdom established a fusion center for all-source analysis of cyber threats and incidents. The new Centre for Cyber Assessment (CCA) was modeled on a similar all-source center MI5 had established for counterterrorism purposes. Though personnel from a variety of agencies staffed the CCA, it was housed, not surprisingly, within GCHQ.[44]

The National Cyber Security Centre

By 2015, much progress thus had been made, particularly on the information-sharing front. Yet the collective impact of malicious cyber activity was continuing to grow and was increasingly occupying the attention of senior policy makers. The head of the OCSIA (the Cabinet Office body established by the 2009 strategy), Matthew Gould, pondered what other steps might help. Gould previously had served as the British ambassador to Israel and had seen firsthand how effectively the Israelis had organized for cybersecurity both within government and in terms of the public-private interface. Notwithstanding the achievements of CERT-UK and CiSP, perhaps more could be done on that front.[45] Relatedly, perhaps the time had come for the government to play a more direct role in improving private-sector defenses. With limited exceptions such as GCHQ's push for telecommunications companies to adopt automated threat detection, the government's efforts to improve private-sector defenses to this point had focused heavily on information sharing, and on voluntary actions more generally. This relatively hands-off approach left it to the private sector, by and large, to determine the nature and scale of its investments in security, and it was becoming apparent that this was not resulting in improvements quickly enough. As then director of GCHQ Robert Hannigan would later explain:

> Any new technology tends not to be developed with safety or security at the front of mind. A combination of government regulation, insurance and self-regulation through market forces tends to put this right over time, the automotive industry in the 20th Century being the obvious example. In cyber security, too much of the burden fell on consumers, whether companies or individuals.[46]

Simply put, there was a market failure of sorts at work. Companies did not internalize the full set of costs inflicted on society due to cybersecurity lapses, and hence did not have strong economic incentives to invest in reducing such harms *ex ante*.[47]

The options for ameliorating such failures are well understood. We see them on display in the context of the auto industry, in fact. One can modify rules of legal liability (substantive or procedural) so as to force companies to internalize more of those societal costs. One can empower a regulator to mandate, directly, that certain interventions be used or procedures followed. Or one can do all of the above. None of these tools is easy to bring to bear, however, given the complicated politics they entail. Relatedly, both risk stifling much-needed innovation if not handled deftly enough. As a result, if a promising alternative approach can be found, one that might provide real systematic improvements without incurring such costs, it can prove highly attractive.

This perhaps explains why the Cameron administration ultimately sought to address the problem of systematically insufficient cybersecurity through another round of institutional innovation, rather than through a major intervention in the form of liability or regulations. Yes, many institutional innovations already had occurred, as we have seen. But an upshot of all this was organizational multiplicity and complexity, and thus uncertainty and coordination challenges. To remedy this, one might consolidate an array of government cybersecurity institutions and functions under the rubric of a single, highly visible, and public-facing entity, one capable of ensuring alignment across these functions and of building a brand to which trust could attach. One might also give such an entity a mandate to take on a more active role in driving specific defensive improvements in the private sector, and resources to take on coordination and operational functions to boot. Thus was born the National Cyber Security Centre (NCSC), with GCHQ's Ciaran Martin as its founding chief executive.[48]

NCSC consolidates many of the organizations we have discussed, including CERT-UK (and, by extension, the CiSP information-sharing system), CCA (the fusion center for cyber-intelligence analysis), and the cybersecurity-specific aspects of CPNI.[49] But where to place NCSC itself?

One option was for it to stand alone as an independent government agency (in the way that the American CIA stands apart from any larger department). Another option would be to have NCSC exist only as a thin layer of bureaucracy for interdepartmental coordination,

superimposed above the incumbent agencies but leaving those agencies where they had been located previously in the organizational chart (akin to America's Office of the Director of National Intelligence). Or it could be embedded within a larger, existing organization (the path the United States followed with what became CISA, within DHS). In the end, that last approach prevailed; NCSC would be a component of GCHQ.

In his speech formally announcing the launch of NCSC (delivered at GCHQ, naturally), Chancellor George Osborne reviewed the accomplishments of the most recent five-year plan for cybersecurity and spelled out key elements of the next one. The new plan would include a resource surge directed at cyber-crime investigations and at the defense of government systems. But most notably, it also would feature the consolidation of a variety of existing defensive functions, and some new ones as well, in the form of the new NCSC. By being placed at GCHQ, Osborne noted, NCSC would be able to "draw on the necessarily secret world-class expertise within this organisation," even as it also developed a public-facing aspect.[50] This hybridization was the not-so-secret sauce driving the NCSC model. As former foreign secretary William Hague later summed up the point:

> The most crucial decision in creating a strong cyber security centre was to place responsibility for it with the appropriate intelligence agency, GCHQ, but simultaneously to make part of its work open and accessible to the population we need to protect. This is an innovative way to develop intelligence work in an age of cyber, which other nations might well wish to follow.[51]

Plainly, this is a significant difference between the NCSC model and the CISA model, as if CISA were not part of DHS but rather NSA. But though the American political and policy environment has no trouble incubating a military organization like USCYBERCOM within NSA, such an approach was never a serious consideration for what became CISA. Wide swaths of the American private sector most certainly would have balked at voluntary participation in programs associated with an NSA-hosted CISA. In the final analysis, there is no better marker of the distinct reception of NSA and GCHQ in their respective societies than the ease with which the new NCSC was placed squarely within the GCHQ organizational fold. Given the long-standing centrality of GCHQ to all of these functions, described above, no one should have been surprised by this.

GCHQ's director later would observe that British businesses, if anything, turned out to appreciate rather than mind that NCSC was ensconced within the most expert of the cyber-relevant parts of government. Ironically, more friction may have arisen from within GCHQ itself, as some found the prospect of interactions with the public jarring, and perhaps also a distraction from more-traditional missions. But, in the end, the affirmative arguments for placing NCSC within GCHQ were numerous and cumulatively compelling. GCHQ is, after all, the best source of cybersecurity expertise across the UK government. And it typically was the first part of government to detect the most significant attacks. Critically, placement at GCHQ also created optimal conditions for persuading foreign

intelligence partners (particularly but not only Five Eyes partners) that they can share information with NCSC without undue risk. Placement of NCSC at GCHQ also signaled seriousness of purpose, while averting potential limitations on GCHQ's support to NCSC that might have arisen had NCSC been placed elsewhere.[52]

Under the leadership of its founding chief executive officer, Ciaran Martin, NCSC quickly became the undisputed focal point for the government's defensive cybersecurity efforts. In many respects, in fact, Martin's founding tenure at NCSC tracked that of his contemporary Chris Krebs at CISA in the United States. Both are personable leaders who took the reins of organizations that had substantial preexisting roots yet needed a new collective identity, and over a period of years both earned positive reputations for their agencies, often running against the grain of the reputations of the larger governments of which they were part.

And the organizations themselves have many parallels. Both have obligations encompassing government systems as well as private critical infrastructure, including the promulgation of defense-relevant advice and threat information. Both also provide an array of security-supporting services, including vulnerability assessments, testing, exercises, and entity-specific technical advising. And both are creative in seeking to identify active technical measures that could be adopted to make the public as a whole, and critical infrastructure in particular, safer (something NCSC does in particular through its "active cyber defence" initiative, which aspires among other things to reduce the impact of "high-volume commodity attacks by stopping them before they reach end users"[53]).

The organizations are by no means identical as a functional matter, however. NCSC's role in relation to coordinating responses to major cyber incidents is far more robust than that of CISA, particularly now that the Biden administration has reestablished a National Security Council post charged with such responsibility, not to mention the passage of legislation creating a new office of National Cyber Director as part of the larger White House bureaucracy. And though the details of NCSC's *operational* defensive functions are less than clear from the public record, they nonetheless must be much broader than those of CISA given CISA's limited authority in that space.[54] In both these senses, we see that the British approach has evolved to a point that is more unified, and better connected to the expertise of its largest and most capable institution (GCHQ), than the American model.

That is, of course, exactly what one might expect given the greater flexibility inherent in the British model of government organization, combined with the British political system's relative comfort with its intelligence services. As Chancellor Osborne stated in his 2015 speech announcing the plan to create NCSC:

> I am clear that the answer to the question "who does cyber?" for the British government is to a very large degree—"GCHQ." . . . GCHQ has a unique role. It is the point of deep expertise for

> the UK government. It has an unmatched understanding of the internet and of how to keep information safe. It is a centre of capability that we cannot duplicate, which must sit at the heart of our cyber security.[55]

That is a set of claims that would be equally true if uttered by an American president with respect to NSA. Yet even in the aftermath of fiascos such as SolarWinds, there remains little if any talk—let alone serious policy and political momentum—about a change in American policy in the direction of the British model.

Before turning to the comparison of American and British approaches to offensive aspects of cybersecurity, a final note is in order. Like the American model, the British model has a long tradition of "light touch" regulation of the private sector, even in the context of critical national infrastructure. More to the point, only a few critical national infrastructure sectors had regulators with relatively strong regulatory authority relevant for cybersecurity. Beyond the nuclear power and financial services sectors, the notional authority of these entities was limited.[56] The beginnings of a shift appeared to emerge in May 2018, though, as the United Kingdom moved to implement the European Union's Network and Information Systems Directive. The implementing rules—known as the NIS Regulations—in theory will "drive change in behaviour and alertness among the operators" who "provide essential services, with an emphasis on ensuring continuity of service."[57] The resulting regulatory interventions may or may not prove significant. Meanwhile, however, a clearly significant shift is on the way for the telecommunications sector thanks to the Telecommunications (Security) Bill. This bill, which is still pending at the time of this writing, will impose a variety of specific security requirements and empower regulators to conduct compliance investigations and impose substantial fines.[58]

ADAPTATION FOR OFFENSIVE FUNCTIONS

From a government perspective, the increasing centrality of the cyber domain constitutes more than just a source of massive risks resulting in the array of defensive functions described above. By the same token, it also gives rise to stunning opportunities for pursuing other public-policy goals, from law enforcement and espionage to armed conflict and covert action. As a result, violating computer security, rather than defending it, at times may become a government policy preference. That, in turn, raises critical questions of institutional and legal design, particularly where the pursuit of such offensive goals comes into direct tension with pursuit of defensive ones. The following comparison of the US and UK "offensive models"—this time conducted side by side with reference to a series of particular offensive functions—illustrates the resulting complexity.

Espionage

The espionage function—that is, stealing secrets to inform planning and decision making—is an area in which the emergence of the cyber domain was not particularly

disruptive for the United States or the United Kingdom. Each country possessed world-class intelligence agencies focused on capturing intelligence through electronic means long before the blossoming of the digital age, and both countries' agencies paid close attention to key advances in computing and encryption (and, indeed, generated many of the most important of those advances). Whatever frictions may have attended the process of reallocating resources, capabilities, and personnel toward the new digital communication and storage systems that emerged over the years, there was never any doubt that NSA and GCHQ would be their countries' respective lead agencies when it came to hacking for espionage purposes, nor any surprise that they would become world-class practitioners of the art.[59]

For the United States, the emergence of hacking as a vector for espionage has not prompted legislative changes. To be sure, the legal architecture for US espionage has evolved considerably over the past two decades, particularly when it comes to SIGINT. But the changes have not been specific to hacking. Several rounds of changes to the Foreign Intelligence Surveillance Act (FISA) have occurred, for example, with the most notable changes involving the creation and tailoring of the "Section 702" system (which enables the US government to compel companies subject to US jurisdiction to cooperate in efforts to locate and access the communications of specific non-US persons located outside the United States for foreign-intelligence purposes). Neither Section 702 nor any other statute attempts to regulate the ability of NSA to conduct hacking outside the United States for espionage purposes.

GCHQ's situation is somewhat different, in that hacking is addressed specifically (if euphemistically) in a somewhat analogous framework. Under pressure from the European Court of Human Rights (ECHR) in the early 1990s, the United Kingdom passed the Intelligence Services Act 1994 (ISA) in order to establish that all of its secret intelligence services, GCHQ included, operated with express parliamentary approval.[60] Notably, ISA's description of GCHQ's activities included "[interference] with . . . equipment" associated with electronic communications.[61] The "equipment interference" (EI) category is widely understood today to encompass hacking, and since 2016, EI has been subject to the Investigatory Powers Act (IPA).[62] Under the IPA, the secretary of state is empowered to issue warrants for GCHQ to carry out EI activities in various ways, subject to oversight from an independent judicial commissioner.[63] The warrant process is obligatory if "there is a British Islands connection."[64] If there is not, the secretary still may opt to employ the warrant procedure, which might be useful should the cooperation of a third party such as a telecommunications company be needed, though this is not obligatory.[65]

The more-interesting changes for espionage-related hacking, for both the United States and the United Kingdom, involve a particular type of institutional innovation. Thanks to the distinctive attributes of hacking as a form of espionage, it eventually became necessary in both countries to develop a novel mechanism for managing a question that almost never

otherwise arises in the espionage setting: should the government undermine its own ability to use certain tools for espionage purposes in order to protect the broader public from others exploiting the vulnerabilities on which those tools depend?

The traditional tools of SIGINT—such as advanced antenna technology—rarely if ever raised such questions. When NSA and GCHQ placed antennae in places that could intercept Soviet military communications, their success usually did not depend on preserving the secrecy of latent vulnerabilities in the systems that enabled such communications. The trick, rather, was to get close enough to effectuate the interception as a matter of physics, and then to overcome whatever encryption might have been used. Even where the collection depended on exploitation of some otherwise undiscovered vulnerability in the underlying system, moreover, it was not likely that that system was one also used by the US and UK governments, let alone their general publics.

All of that is reversed in the case of hacking. Or at least, hacking raises the critical question: might the greater national interest sometimes lie in making sure that vendors become aware of (and hopefully try to patch) vulnerabilities, rather than keeping quiet about the vulnerabilities in order to exploit them for espionage purposes? Over time, both the US and UK governments have determined that this question demands an institutionalized response. The result, in both countries, was the creation of an interagency "vulnerability equities process," or VEP, in which the interests of intelligence collection are weighed, systematically, against competing considerations in a bureaucratic process that includes input from entities outside the intelligence community.[66] For both the United States and the United Kingdom, further evolution in this space is very likely.

Of course, intelligence agencies are not the only government entities with a stake in preserving the viability of a vulnerability. The ability to hack is increasingly important for other government purposes.

Armed Conflict

There was a time, not long ago, when it was thought newsworthy when a government avowed that its military had hacking capabilities. Yet there was never any real doubt that militaries would establish such capabilities. Electronic warfare has been a staple of armed conflict ever since militaries began making use of electricity-based technologies. In today's world, computers have become essential for a range of military functions, with everything from command-and-control across military formations to supply chains to the operation of weapons systems depending on them. Every military must mind the cybersecurity aspects of these systems, just as every military must aspire to overcome an enemy's cyber defenses by hacking them in order to understand, disrupt, manipulate, or even destroy adversary capabilities during armed conflict.

Like other modern militaries, both the United States and the United Kingdom accordingly have developed their offensive military cyber capabilities in addition to their defensive ones. But they have not done so in precisely the same way, as an institutional matter.

For every military, the need to have offensive cyber capabilities in the event of armed conflict presents an interesting institutional design challenge. There are at least two reasons for this. First, the capabilities that make for a talented hacker are different in kind from those traditionally prized in the context of run-of-the-mill military recruitment and training, more so than with other domains of military operations. This suggests the utility of developing distinct institutional processes for recruitment, training, and career development of cyber-capable soldiers. Second, sophisticated hacking operations at least sometimes call for expensive or scarce computing infrastructure that militaries normally would not develop and sustain. This too suggests the need for something distinctive, just as is the case for sea, air, and now space operations.

In both the United States and the United Kingdom, it did not escape notice that world-class capabilities of the sort that militaries could use, in terms of personnel and supporting infrastructure, already existed at NSA and GCHQ, respectively. In both contexts, military officials accordingly were drawn to the possibility of somehow drafting off of those capabilities, rather than attempting to generate them from scratch. And that is exactly what happened, though the two countries went about things in distinct ways.

As described earlier in the section on defense, the United States chose an incubation model. As related by Michael Warner, the US established USCYBERCOM as a distinct military organization, yes, but embedded it in every practical sense of the word alongside NSA at Fort Meade.[67] With shared personnel and infrastructure, and even a dual-hatted leader, USCYBERCOM to this day is formally a purely military organization that, functionally, shares substantial DNA with the intelligence community. And though the original expectation of the incubation model was for USCYBERCOM eventually to emerge from NSA's shadow, the moment of separation seems to continually recede.[68]

This is not just because Congress has enacted legislation precluding formal separation until the secretary of defense certifies that USCYBERCOM has reached certain sustainability benchmarks (though these benchmarks in fact have not been reached as of the time of this writing).[69] There are many who feel that the US has created, however unintentionally, an attractive hybrid model providing an optimal degree of capability and efficiency, one that ensures USCYBERCOM can punch above its weight. Defenders also contend that this model inherently ensures thoughtful consideration of competing equities when the benefits that might flow from disrupting an adversary's system threaten to undermine those that come instead from simply collecting intelligence from within that system.

Others disagree. Critics have argued that separation is needed if ever USCYBERCOM is to reach its full potential, much as training wheels must come off a bicycle. And critics also have inverted the equities-deconfliction point, arguing that the current arrangement unduly empowers NSA to protect its intelligence-collection equities (which typically will favor monitoring rather than disruption of adversary systems) at the expense of the military operational equities that USCYBERCOM might otherwise prioritize.

This line of argument came to a head, publicly, amidst the war against the Islamic State (ISIS). ISIS was making use of the online environment for both command-and-control and external recruitment and fundraising efforts. Then secretary of defense Ash Carter became concerned that USCYBERCOM was not acting aggressively enough to disrupt ISIS systems, perhaps because intelligence-collection equities were receiving too much consideration. Ultimately, USCYBERCOM did begin conducting disruption operations with greater frequency, under the rubric of Operation Glowing Symphony. The results disappointed some observers (ISIS was able to reconstitute at least some functionality relatively quickly). Supporters of the status quo saw this as evidence that intelligence-collection equities should indeed often prevail, and thus that the current arrangement should be preserved. Critics concluded that, on the contrary, this was evidence of the need to break the mold so that USCYBERCOM might develop more-robust capabilities and have an easier time making use of them.

Notably, certain aspects of Operation Glowing Symphony drew attention to critical and hotly contested questions at the intersection of international law, international relations, and the interagency tensions inherent in a model that maintains formal separation between military and intelligence-agency authorities. Servers used by ISIS for its communications, particularly their public-facing recruitment efforts, were not always (or even often) located inside the zone of active hostilities in Syria and Iraq. As a result, some counter-ISIS cyber operations required accessing systems that were physically located in third-party countries, including Germany. The State Department, CIA, and FBI were concerned that such operations, if conducted without the consent of the country in question, might result in backlash impacting bilateral cooperation on other fronts. Objections also may have been raised on international-law grounds on the basis of a claim that operating on those servers without consent from the country involved might violate that country's sovereignty.

On the domestic legal front, moreover, it might also be argued that USCYBERCOM, unlike the CIA, lacks authority to conduct such third-country operations when they violate international law.[70] The Pentagon countered such claims by asserting that the planned operations would have no significant collateral effects and, in any event, that its existing authorities sufficed to cover nonconsensual operations such as these. It appears likely that the Pentagon may also have disputed that there is a general international-law rule of sovereignty as such, as distinct from the clearly established rules concerning the "use of force" and coercive interventions in international affairs.[71]

A significant period of time elapsed as the interagency debate played out. In the end, it seems a compromise emerged. The United States gave advance notice to as many as fifteen countries that it might seek to execute such operations. But it did not actually make consent from these countries a condition for conducting those operations. Ultimately, USCYBERCOM appears to have conducted operations in five or six of them, including Germany, without host-state consent.[72]

Given this breakthrough for USCYBERCOM, the United States may at some point conclude that its current hybrid model is, in fact, an attractive end state rather than just a transitional framework. Whatever its fate, though, it was never the only institutional pathway for enabling armed forces to get the benefit of intelligence-agency capabilities. The UK experience illustrates how this same general goal can be pursued in a more direct and integrated, though smaller-scale, way.

Unlike NSA's relationship to the Department of Defense, GCHQ is not a component of the Ministry of Defence (MoD). But like NSA, GCHQ nonetheless has always played a critical role in support of combat operations (as its famous World War II exploits remind us). Traditionally, this role centered on SIGINT collection and protection of military communications. This had implications for the United Kingdom as it became clear over time that cyberspace was becoming an important domain for actual operations during armed conflict, and not just a medium for SIGINT. Like the United States, the United Kingdom faced an institutional design choice. It could seek to build up an independent capability within the military to conduct offensive cyber operations, either from scratch or by following the American incubation model described above. Or it could just allocate this function to GCHQ, matching the new mission with existing expertise and capacity.

As former GCHQ director Hannigan has explained, practical considerations compelled selection of the GCHQ option. "In governance and structural terms," Hannigan writes, "we made an early decision not to imitate the US model of a separate Cyber Command alongside the NSA. Given the scale of the UK system, duplication was not viable or affordable, and an integrated military-civilian model seemed preferable."[73] Even if resource constraints had been otherwise, moreover, the case for the GCHQ model was strong. "The skills and access necessary to do this resided almost exclusively in GCHQ," Hannigan writes.[74] And since "support for military operations has always been a key part of GCHQ's mission," GCHQ already employed "a large number of military officers as part of the workforce," a consideration that smoothed the way for further integration.[75] Nor did GCHQ require any new legal authorization in order to take on this offensive role. Unlike NSA, GCHQ "had always had the legal authority to mount offensive cyber operations," and in fact it already had crossed this particular Rubicon "under ministerial authorization in limited cases."[76]

This combination of efficiency, efficacy, and authority ultimately led to the formalization, in 2014, of the National Offensive Cyber Programme (NOCP). It had been clear since

the year before that something was afoot, as then defence secretary Philip Hammond in 2013 had avowed the United Kingdom's development of "a full spectrum military cyber capability, including a strike capability."[77] What had not been clear was the institutional arrangement that would make this possible. And so it was significant when Chancellor Osborne in his 2015 speech at GCHQ explained that NOCP "is a partnership between the Ministry of Defence and GCHQ, harnessing the skills and talents of both organisations to deliver the tools, techniques and tradecraft required for the UK to establish a world class capability."[78] It was not long before that capacity was put into practice. Just as USCYBERCOM eventually went into action against Islamic State assets via Operation Glowing Symphony, so too did GCHQ, in partnership with MoD. Years later, UK officials would avow that the organizations began conducting disruption operations against the Islamic State in 2016. GCHQ's then director, Jeremy Fleming, disclosed in his first public speech that they conducted operations that included, apparently, both disruption and manipulation of ISIS's online communications, degrading both operations and propaganda. This work made it "almost impossible [for ISIS] to spread their hate online, to use their normal channels to spread their rhetoric, or trust their publications."[79] The impacts were not just functional, either. Fleming disclosed that some of the operations "destroyed equipment and networks."[80] Later disclosures elaborated that these operations disrupted ISIS control over their drones and at times shut down or altered cell phone and laptop communications for ISIS fighters in the field, including sending false orders that would lead the fighters into an ambush.[81]

NOCP was not an interagency end state, however. Word began to circulate that the GCHQ-MoD partnership would take on a more formal institutional structure, with a greater emphasis on "jointness." One early account described plans for a two-thousand-member task force combining GCHQ and MoD personnel, and another described ongoing debates about whether the new entity would be directed by a GCHQ figure, a military officer, or perhaps even both in rotation.[82]

By 2019, it was reported that the new strategic partnership between GCHQ and MoD was to be known as the National Cyber Force, or NCF, and Defence Secretary Ben Wallace confirmed this in a speech that year.[83] And then came the announcement from Prime Minister Johnson quoted at the opening of this paper: NCF was now in operation, and indeed had been since April 2020. Though its dedicated personnel at that time apparently numbered around three hundred, plans called for it to expand to three thousand over the following ten years.[84] Along with GCHQ and MoD, moreover, MI6 (the Secret Intelligence Service, which from a US perspective is analogous to the CIA) is a participating organization as well. A longtime GCHQ official is at the helm, at least for now.[85]

In the final analysis, NCF is a manifestation of the same hybridization trends that led to the incubation model for USCYBERCOM in the United States. It is far more thoroughly integrated than its US cousin, however—more of a true hybrid. As Rory Cormac recently

observed, NCF illustrates how "the United Kingdom takes a whole-of-government approach, without the distinctions made in the United States between covert action and special military operations."[86] The resulting "fuzziness," Cormac notes, "allows a more flexible and nimble response to fast-moving threats, free from too many bureaucratic constraints."[87] We see this with NCF even at the level of ministerial accountability, moreover, as (in contrast to NCSC) both the defence and foreign secretaries have purview over NCF's affairs (though the particulars as to when the approval of both or either might be required for certain types of operations is not clear from the public record).[88]

As we shall see in the final section below, this has implications for the frictions these entities encounter with respect to a growing segment of their respective missions.

Disrupting Malicious Cyber Activity Apart from Armed Conflict

Neither the United States nor the United Kingdom went down these complex institutional paths strictly to establish and enhance cyber capabilities to be used in combat. In both cases, there is a separate motivating force in play.

From information operations to ransomware, the strategic significance of harmful cyber activities occurring outside the context of armed conflict is on the rise, including not just activities that inflict harm in the cyber domain itself, but also those that depend on the cyber domain as a vector for inflicting noncyber harms. This has spurred attempts to elevate defenses, as well as efforts to impose costs on attackers via prosecution, sanctions, and the like. Too often defensive improvements seem not to keep pace, however, and the perpetrators cannot be reached effectively with punitive tools. And so some governments—including those of the United States and the United Kingdom—have turned their attention to the possibility of using cyber means to disrupt these harmful activities at their source.

The stories of USCYBERCOM and the NCF cannot be fully understood apart from this. Independent of their combat missions, both entities have missions that call for what the Americans describe as "defending forward" and the British describe as "offensive" operations—that is, operations designed to cause disruptive effects in adversary networks in order to halt or forestall malicious activity. Those missions raise critical questions of institutional design and legal architecture.

For the United Kingdom, it is proving relatively easy to address the institutional issues this mission set raises, thanks to the fully hybridized nature of first NOCP and now NCF. After all, neither was ever intended to be limited to combat-related operations. On the contrary, descriptions of their functions have routinely emphasized noncombat scenarios. When discussing the need for NCF, for example, General Sir Patrick Sanders of Strategic Command noted that foreign governments have been tearing at "the fabric of society" through

disinformation operations leveraging social media. "Offensive cyber," he concluded, "is unquestionably one of the tools" governments need to respond to such attacks on "the cohesion of society and . . . our democratic processes."[89]

An earlier report in the *Times* similarly anticipated that NCF would respond to foreign disinformation campaigns by hacking foreign systems to "remove fake news."[90] Nor would NCF's role be limited to responding to the malicious activities of state actors. As part of the formal NCF rollout in late 2020, Foreign Secretary Dominic Raab emphasized that NCF would operate not only against hostile foreign states and terrorists, but also against certain crime challenges such as "online child abuse."[91] Prime Minister Johnson has underscored the point as well, stating that NCF's objectives will include operations against "criminal gangs," while former NCSC chief executive Ciaran Martin notes that the UK's offensive capabilities have "always included an emphasis on disrupting organized cyber crime."[92] NCF's remit, in short, is comparatively broad in this respect, encompassing both state-sponsored and nonstate threats that might effectively be mitigated through disruptive operations conducted in the cyber domain.[93]

These examples of activities NCF might respond to do not all fall readily into a single traditional threat category such as "intelligence" or "crime." Rather, they share in common a functional characteristic: they emanate from activity that is sourced overseas in physical locations that have proven resistant to traditional means of response (such as diplomatic efforts to persuade host states to intervene effectively to stop the harms), but which depend on online systems and hence are vulnerable to disruption in that domain. NCF as a practical matter is well suited to take advantage of that vulnerability, in terms of both its technical capabilities and its hybrid nature. Since the UK model does not stand on categorical formalities in the same way as does the US model, moreover, NCF is unlikely to face objections on grounds of exceeding the scope of its institutional role.

It does not follow that NCF's role in such missions raises no concerns, of course. Conrad Prince, for example, has pointed out that the uncertain scope of NCF's "offensive" mission makes it more difficult to have an effective discussion of the ethical and legal boundaries that may govern NCF's operations in such unconventional settings.[94] The legal and ethical issues are complex enough with respect to cyber operations in the context of armed conflict, after all. Once one moves beyond that context, they grow murkier. Without a firm grasp of what the UK government considers out of scope for NCF in the first place, it is hard to have a serious conversation about such matters.

This problem may be less significant than it first appears, however. Much depends on the connotations of the terms "offense" and "offensive." Taken for all they are worth, those terms imply that NCF might even act as an aggressor, initiating malicious online activity rather than using online means to disrupt malicious activity initiated by an adversary. It seems unlikely, however, that NCF's mission actually extends that far. The examples of

NCF missions that ministers and others have cited all appear to involve "offense" only in the much narrower, tactical sense in which any act of hacking might be described as offensive (i.e., because it involves breaching a system's security).

There is a world of difference between hacking a system in order to cause harm in the first instance and, instead, doing it to stop someone else from causing ongoing harm. The latter is, in the sense that counts most, a *defensive* use of hacking.[95] All the examples given for NCF are defensive ones in that sense, fortunately. It is worth noting, too, that former GCHQ director Hannigan has expressly cautioned against the United Kingdom engaging in what would instead be genuinely offensive noncombat cyber operations, pointing out that the United Kingdom is asymmetrically vulnerable in the cyber domain and that such activities might be unlawful and inconsistent with the United Kingdom's values.[96]

Those who follow US cyber strategy should recognize in all of this a close parallel to the often-confusing debates associated with the "defend forward" model adopted by USCYBERCOM in recent years.[97] This is no coincidence. The US model faces the same category-blurring threats as does the British one, and likewise sees the attraction of conducting disruption operations inside adversary networks, given the poor track record of more-traditional modes of response. When USCYBERCOM speaks of defending forward, this encompasses an array of operational circumstances including operating by consent within the networks of allies in a wholly defensive capacity. But it also encompasses "red space" operations to disrupt malicious activity at its overseas source in some circumstances.

The analogy to NCF's circumstance is by no means complete, though. As an initial matter, USCYBERCOM also has conventional defensive responsibilities concerning the US military's own system, whereas NCF has no comparable role. More interesting for our purposes, however, is the comparative degree of hybridization between the two approaches. Questions of institutional scope, as we have seen, are far more consequential in the US model, and USCYBERCOM is not institutionally hybridized to the same degree as NCF. USCYBERCOM, as a result, already has faced considerable friction and likely will experience more of the same in the years ahead.

As described in my separate paper in this series on the domestic legal architecture of US military cyber operations, USCYBERCOM initially faced objections that neither it nor the Defense Department in general had affirmative authority to conduct cyber operations abroad outside the context of armed conflict.[98] Relatedly, some objected that the operations it sought to conduct might have to be categorized as "covert action" for purposes of the complicated statutory oversight frameworks usually associated with the CIA, meaning either that USCYBERCOM should not conduct them at all or else that it would have to submit to the covert-action oversight system, including the requirement of written presidential authorizations, if it did so.

Ultimately, Congress over a period of years took note of and largely eliminated each of these objections through a series of statutory amendments. As a result, USCYBERCOM today enjoys relatively clear affirmative authority to engage in out-of-network operations in at least some circumstances. This authority is clearest in circumstances involving Russia, China, Iran, and North Korea, for Congress has enacted an express authorization for cyber operations to disrupt malicious campaigns attributable to those states in particular (subject to certain conditions).[99] Where attribution does not run to one of those states, the picture necessarily is more complicated given the absence of an on-point statutory authorization. In such cases, authority to act still may exist—indeed, it plainly would exist given a sufficient threat to the United States—but it must be inferred from a combination of the inherent national self-defense authorities the Constitution confers on the president and other, more general statutes. This, in turn, suggests that it likely is more difficult—perhaps far more difficult—for USCYBERCOM than for NCF to engage in disruption operations involving, say, nonstate actors engaged in crime (though recent reports of a USCYBERCOM operation targeting the TrickBot network illustrates that here, too, the US and UK models may be converging in practice).

A final comparison concerns the international legal frameworks that govern such "offensive" operations outside the context of armed conflict. Here we find another possible point of departure between the US and UK models.

Both the United States and the United Kingdom accept, naturally, that international law as a default rule prohibits the "use of force" in international affairs as well as coercive "interventions" into the *domaine réservé* of other states. Hard questions abound regarding just which activities would implicate those rules, but the existence of the rules themselves is settled. It is different, however, with respect to the proposition that there also is a rule of international law forbidding interference with the "sovereignty" of other states below the threshold of coercive intervention. The US and UK governments currently seem to adhere to a similar understanding on this issue, but there is reason to wonder whether that might change.

The position of the United Kingdom on the sovereignty question is clear. In a 2018 address at Chatham House, Attorney General Jeremy Wright raised the question of whether sovereignty should be recognized as a rule of international law entailing prohibitions beyond those already associated with the well-recognized rules involving the use of force and coercive intervention. He recognized that some advocates "have sought to argue for the existence of a cyber specific rule of a 'violation of territorial sovereignty' in relation to interference in the computer networks of another state without its consent."[100] Wright responded by acknowledging that the *principle* of sovereignty "is of course fundamental to the international rules-based system."[101] It was not itself a stand-alone rule of international law, however. "I am not persuaded," he explained, "that we cannot currently extrapolate from that general principle a specific rule or additional prohibition for cyber activity

beyond that of a prohibited intervention."[102] Accordingly, the "UK Government's position is therefore that there is no such rule as a matter of current international law."[103] Combined with the integration of GCHQ, MoD, and MI6 elements into NCF, this clarity on the international legal framework paves the way for NCF to operate on a nonconsensual basis if and when it takes action on systems that happen to be physically located in other countries.

Matters are not quite as clear with the United States, though for the time being it appears that the US approach does track that of the United Kingdom.

The US government has never quite offered an unambiguous position on the sovereignty question as such, at least not on a par with Attorney General Wright's speech. In 2016, State Department Legal Adviser Brian Egan stated that "cyber operations involving computers or other networked devices located on another State's territory do not constitute a *per se* violation of international law," and that "precisely when a non-consensual cyber operation violates the sovereignty of another State is a question lawyers within the US government continue to study carefully, and it is one that ultimately will be resolved through the practice and opinio juris of States."[104] This left open the possibility that the United States might recognize, at some point, at least some form of sovereignty rule extending beyond the concept of coercive intervention, with some nonconsensual cyber operations perhaps crossing that line even if not all did. Then, in early 2020, Defense Department General Counsel Paul Ney gave a speech at USCYBERCOM's annual legal conference in which he took up this issue. Ney first restated Egan's position, arguing that "there is not sufficiently widespread and consistent State practice resulting from a sense of legal obligation to conclude that customary international law generally prohibits such non-consensual cyber operations in another State's territory."[105] Ney then went a step further, arguing that USCYBERCOM's "defend forward" model, in particular, "comports with our obligations under international law and our commitment to the rules-based international order."[106] It was not quite the same thing as denying that there exists any rule of sovereignty as such, and Ney conspicuously emphasized that his office's position "shares similarities with the view expressed by the U.K. Government in 2018" rather than simply asserting full agreement with that view. Nor was it a position for the US government as a whole, meaning that other agencies (such as the State Department) might not agree with all he had said. But it was at least an assertion that, as far as DoD lawyers were concerned, there was no international-law constraint that would be violated by the particular range of activities contemplated by the "defend forward" model.

Perhaps over time the United States will move closer to the clarity of the UK position. Then again, it is possible either might move in the opposite direction. As described by Jack Goldsmith and Alex Loomis in their paper in this series, there are those who take the position that there is indeed a distinct international-law rule of sovereignty, and among them are some who contend that this rule would indeed be violated by at least

some nonconsensual cyber operations that might take place outside the context of armed conflict.[107] This is, for example, the position taken by the scholars who produced the *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*.[108] Goldsmith and Loomis offer a sharp critique of that position, but the fact remains that a number of states have endorsed a similar view.[109]

Were the United States to make such a shift, it might have complicated institutional implications. USCYBERCOM's operations are not subject to the US domestic legal framework for "covert action."[110] In some respects that may be liberating, but in one notable respect it is otherwise. Federal law provides that covert action must comply with the Constitution and statutes of the United States, but not necessarily with international law.[111] When the CIA conducts a cyber operation under color of its "Title 50" covert action authorities, consequently, it would not necessarily matter (from a US domestic-law perspective, at least) if it violated a supposed international-law rule of sovereignty. USCYBERCOM's operations ordinarily would not constitute covert action, however, thanks to a series of interventions by Congress in recent years. Between that consideration and the general DoD policy of international-law compliance, then, a US shift in favor of a rule of sovereignty might well result in genuine constraints on USCYBERCOM's freedom of action.

A similar shift in legal policy by the United Kingdom might have a still-broader impact. Whereas the American model contemplates (however quietly) the prospect of activities that might violate international law (so long as they are conducted under the formal covert-action rubric), it is far from obvious that the same is true in the British system. When British officials speak about the relevance of international law to cyber operations, as did then attorney general Wright in his 2018 address, the emphasis is on the obligation to states to ensure that their cyber operations are "carried out in accordance with international law."[112] Of course, American officials say similar things, but, as noted above, the American statutory framework for covert action paves the way for circumvention in that limited context. There is no comparable British domestic-law pathway, however. This perhaps helps us understand why the British have been at greater pains than the Americans to state their views on just where the international-law boundaries run—not to mention why Wright so clearly rejected the idea that sovereignty should be recognized as a rule rather than just a principle of international law. As Ashley Deeks has written:

> Assertions that its intelligence activities comply with UK international legal obligations (including the ECHR) appear to compel the UK to take aggressive legal interpretations of international law itself, so as to cabin its scope in a way that is compatible with the imperatives of its IC.[113]

A change of policy on the sovereignty question would have government-wide implications for the United Kingdom, then, not just for MoD.

CONCLUSION

As in so many other respects, there is more that unites the United States and the United Kingdom than separates them when it comes to questions of cyber policies, laws, and institutions. The gradual processes through which both have adapted to the growing strategic significance of the cyber domain in terms of defensive liabilities and offensive opportunities bear this out. With comparable legal systems, rule-of-law commitments, and legacy institutional structures, as well as generations of close collaboration in military and intelligence matters, this should come as no surprise.

Yet the pathways followed by London and Washington have not been identical. It is not just that the United States brings disproportionate resources to bear when developing and supporting its security-related institutions (a proposition that rings true with USCYBERCOM much more so than for CISA, it should be noted). There are, too, notable differences in their respective societies, including ones that manifest in their respective approaches to structuring government institutions. The United Kingdom does not share the US predilection for compartmentalized lines of formal authority. And GCHQ involvement in matters beyond traditional overseas intelligence collection does not appear to set off quite the same antibodies in the body politic of the United Kingdom as would NSA or USCYBERCOM in the United States.[114]

The upshot of it all is that we see a strong degree of convergence between the United States and the United Kingdom, especially from the purely defensive perspective. But we also see important elements of variation, above all in terms of the degree to which the two governments integrate their most capable operators—NSA and GCHQ—into their nonintelligence activities. Time may demonstrate that one model or the other is superior in practice as a general rule. More likely, though, it will instead teach that there are moments and contexts that favor both, with no one set of institutional solutions always ideal.

NOTES

1 Hon. Boris Johnson MP, U.K. Prime Minister, Statement to the House on the Integrated Review (Nov. 19, 2020).

2 Hon. Ben Wallace MP, U.K. Def. Sec'y, Ministry of Def., Address at the NATO Parliamentary Assembly (Oct. 14, 2019) ("The UK will soon solidify plans for a National Cyber Force to ensure a stronger presence in the new contested frontier.").

3 Fred M. Kaplan, Dark Territory: The Secret History of Cyber War 1–2 (2016).

4 *See* Thomas L. Burns, Ctr. for Cryptologic History, Nat'l Sec. Agency, The Quest for Cryptologic Centralization and the Establishment of NSA: 1940–1952, at 2 (2005).

5 Kaplan, *supra* note 3, at 18–19.

6 *Id.* at 20, 35; *see also* The White House Office, National Security Directive 42: National Policy for the Security of National Security Telecommunications and Information Systems (1990); National Security

Decision Directive 145: National Policy on Telecommunications and Automated Information Systems Security (1984).

7 Clifford Stoll, The Cuckoo's Egg (1989).

8 Kaplan, *supra* note 3, at 71.

9 *Id.* at 81–84.

10 Michael Warner, US Cyber Command's First Decade 4–5 (Hoover Inst., Aegis Series Paper No. 2008, 2020).

11 Kaplan, *supra* note 3, at 100–101.

12 Federal Information Security Management Act of 2002, Pub. L. No. 107-347, 116 Stat. 2899 (codified as amended at 44 U.S.C. §§ 3551 to 3559 (2018)).

13 For a discussion of EINSTEIN's origins and subsequent evolution, *see* Steven M. Bellovin, Scott O. Bradner, Whitfield Diffie, Susan Landau, and Jennifer Rexford, *Can It Really Work? Problems with Extending EINSTEIN 3 to Critical Infrastructure*, 3 Harvard National Security Journal 1 (2011).

14 44 U.S.C. § 3553 (2018).

15 *See* Cybersecurity and Infrastructure Security Agency, Services Catalog (2020).

16 National Defense Authorization Act for Fiscal Year 2021, Pub. L. No. 116-283, § 1705, 134 Stat. 3388 (2021).

17 *Security in Cyberspace: Hearing Before the Permanent Subcomm. on Investigations*, 104th Cong. 43 (1996) (statement of the minority staff).

18 President's Commission on Critical Infrastructure Protection, Critical Foundations: Protecting America's Infrastructures 23 (1997).

19 The White House Office, Presidential Decision Directive 63—Critical Infrastructure Protection (1998).

20 Kaplan observes that PDD-63's lead author, Richard Clarke, believed that sufficient progress would not be made without imposing regulatory mandates on CI owners. "Clinton's economic advisers strenuously opposed the idea," however, "arguing that regulations would distort the free market and impede innovation." Kaplan, *supra* note 3, at 100.

21 The White House Office, The National Strategy to Secure Cyberspace 22 (2003).

22 Exec. Order No. 13636, 78 Fed. Reg. 11739 (2013); The White House Office, Presidential Policy Directive 21—Critical Infrastructure Security and Resilience (2013).

23 Exec. Order No. 13636, 78 Fed. Reg. 11739 (2013).

24 *Id.*

25 Cybersecurity Information Sharing Act of 2015, Pub. L. No. 114-113, §§ 101–407, 129 Stat. 2242, 2936–2985 (codified as amended at 6 U.S.C. §§ 1501 to 1533 (2018)).

26 Press Release, White House Office of the Press Sec'y, Fact Sheet: Cybersecurity National Action Plan (Feb. 9, 2016).

27 Exec. Order No. 13800, 82 Fed. Reg. 22391 (2017).

28 Richard J. Aldrich, GCHQ: The Uncensored Story of Britain's Most Secret Intelligence Agency 486–508 (2010).

29 *Id.* at 488.

30 *Id.*

31 *Id.* at 488–89.

32 *See* Tony Proctor, *The Development of Warning, Advice and Reporting Points (WARPs) in UK National Infrastructure*, *in* Critical Information Infrastructure Security 164, 167 (Bologna, Hämmerli, Gritzalis, and Wolthusen eds., 2011).

33 *See* 661 Parl Deb HL (5th ser.) (2004) col. WA 20 (UK); *see also, e.g.*, Eric Byers, John Karsch, and Joel Carter, *Good Practice Guide: Firewall Deployment for SCADA and Process Control Networks*, Centre for the Protection of National Infrastructure (Feb. 15, 2005) (updating a good practice guide previously published by the National Infrastructure Security Co-ordination Centre).

34 Ciaran Martin, Cyber as Intelligence Contest: The Example of the United Kingdom (manuscript on file with author), at 2, n.2. Robert Hannigan, who served as GCHQ's director from 2014 to 2017, notes that CESG historically was seen as "secondary and unglamorous in comparison to signals intelligence gathering," and that "outside a core group of dedicated experts, many GCHQ staff regarded a posting to the CESG as a step backwards or downwards" during that earlier period. Robert Hannigan, *Organising a Government for Cyber: The Creation of the UK's National Cyber Security Centre*, Royal United Servs. Inst. for Def. and Security Stud. 4–5 (Feb. 2019).

35 *Id.* at 4.

36 Cabinet Office, Cyber Security Strategy of the United Kingdom: Safety, Security and Resilience in Cyber Space, 2009, Cm. 7642 (UK).

37 *See id.* at 4–5, 17.

38 *See id.*; Hannigan, *supra* note 34, at 4.

39 Cabinet Office, The UK Cyber Security Strategy: Protecting and Promoting the UK in a Digital World, 2011 (UK).

40 *See* Stuart Murdoch and Nick Leaver, *Anonymity vs. Trust in Cyber-Security Collaboration*, *in* WISCS '15: Proceedings of the 2nd ACM Workshop on Info. Sharing and Collaborative Sec. 27, 28 (Oct. 2015); Hannigan, *supra* note 34, at 10.

41 Hon. George Osborne, Chancellor, HM Treasury, Chancellor's Speech to GCHQ on Cyber Security (Nov. 17, 2015); Hannigan, *supra* note 34, at 8.

42 Unfortunately, that same phrase for many observers (particularly in the United States) has a distinct connotation associated with the scenario in which a hacking victim retaliates with an out-of-network operation against the attacker; that is not the British usage. *See* Martin, *supra* note 34, at 8 (observing this distinction); John Strand, *Active Defense, Offensive Countermeasures and Hacking Back*, Black Hat (Aug. 2018), https://www.blackhat.com/us-18/training/active-defense-offensive-countermeasures-and-hacking-back.html (offering a course on "active defense" at Black Hat USA 2018).

43 Press Release, Cabinet Off. & Hon. Lord Maude of Horsham, UK Launches First National CERT (Mar. 31, 2014).

44 Hannigan, *supra* note 34, at 10. CERT-UK, notably, was housed in the Cabinet Office rather than GCHQ or any other specific agency. *See* Martin, *supra* note 34, at 4.

45 *Id.* at 13. Hannigan also cites the leadership of Chancellor George Osborne, who at that time headed the cabinet committee responsible for cyber matters.

46 *Id*.

47 Ciaran Martin, Chief Executive, National Cyber Security Centre, Speech in Belfast (Oct. 20, 2017).

48 Hannigan, *supra* note 34, at 13–14. In addition to Hannigan's speech, those interested in the origins of the NCSC should read the excellent account forthcoming from Ciaran Martin. *See* Martin, *supra* note 34.

49 *Id.* at 14.

50 Osborne, *supra* note 41.

51 William Hague, *Foreword*, to Hannigan, *supra* note 34, at vii.

52 Hannigan, *supra* note 34, at 14–15.

53 Joint Committee on National Security Strategy, Cyber Security of the UK's Critical National Infrastructure, 2017–19, HL 222 & HC 1708, at 20 [hereinafter Joint Committee Report]. Ciaran Martin has noted that the creators of NCSC wanted the organization to be more than just a reorganization of existing entities, and in particular to have fresh operationally relevant capacities such as this. *See* Ciaran Martin, Director-General, Cyber at Government Communications Headquarters, and Chief Executive, National Cyber Security Centre, Speech at the Billington Cyber Security Summit: A New Approach for Cyber Security in the UK (Sep. 13, 2016). Toward the latter end, Ian Levy developed a task list involving a dozen technical advances to be pursued under the general brand of "active cyber defence," including pursuing changes to the implementation of Border Gateway Protocol, requiring Domain-Based Message Authentication, Reporting and Conformance (DMARC) for government, working with private-sector partners to take down malicious domains, promoting DNS filtering, and offering web-vulnerability scanning services to government entities. *See* Ian Levy, *Active Cyber Defence—Tackling Cyber Attacks on the UK*, National Cyber Security Centre (Nov. 1, 2016); Hannigan, *supra* note 34, Appendix II at 40–42; *see also* HM Government, Prospectus Introducing the National Cyber Security Centre.

54 Hannigan, *supra* note 34, at 16, 21–23, 34.

55 Osborne, *supra* note 41.

56 Joint Committee Report, *supra* note 53, at 26.

57 *Id.* at 23–24.

58 Explanatory materials are available at https://www.gov.uk/government/collections/telecommunications-security-bill.

59 That is not to say they are the only agencies that perform intelligence collection with cyber means for their respective governments. The public record yields little, however, about how the CIA and MI6 operate in the cyber domain.

60 *See* Aldrich, *supra* note 28, at 484.

61 *See* Intelligence Services Act 1994, c. 13, § 3(1)(a) (Eng.) [hereinafter ISA].

62 For the EI category, *see* The Home Office, Investigatory Powers Bill Factsheet: Targeted Equipment Interference, 2015, at 1 (UK) ("Equipment interference (EI), sometimes referred to as computer network exploitation, is the power to obtain a variety of data from equipment. This includes traditional computers or computer-like devices. . . . EI can be carried out either remotely or by physically interacting with equipment.").

63 *See* Investigatory Powers Act 2016, c. 25, §§ 13, 99–135, 176–198 (Eng.).

64 *See id.* at § 13.

65 *Id.*

66 *See* Ian Levy, *Equities Process*, National Cyber Security Centre (Nov. 29, 2018) (providing a frank account of NCSC's equities process). For a comparable overview of the US model, *see* Press Release, White House Office, Fact Sheet: Vulnerabilities Equities Process (Nov. 2017).

67 Warner, *supra* note 10.

68 There was a half-baked attempt to rush through a formal separation of NSA and USCYBERCOM during the waning days of the Trump administration. But that bid collapsed in the face of congressional objections and the fact that a federal statute forbids separation unless and until such time as the secretary of defense certifies in writing that such a move would not undermine USCYBERCOM's operational capabilities and that an adequate

equities-deconfliction process has been put in place. Thus, as of the time of this writing, the incubator-based hybrid model employed by the US remains as it was.

69 *See* National Defense Authorization Act for Fiscal Year 2017, Pub. L. No. 114-328, § 1642, 130 Stat. 2000, 2601 (2016).

70 Under the relevant aspects of Title 50 of the US Code, activities constituting "covert action" must comply with the US Constitution and federal statutes, but not international law as such. That subtle but significant provision does not extend to military operations (unless they qualify as "covert action" in a statutory sense), and the Pentagon at any rate has a policy of conducting all operations in accordance with international law. *See* Robert Chesney, *Title 10 and Title 50 Issues When Computer Network Operations Impact Third Countries*, Lawfare (Apr. 12, 2018).

71 *See* Hon. Paul C. Ney Jr., Speech at U.S. Cyber Command Legal Conference (Mar. 2, 2020).

72 Ellen Nakashima, *U.S. Military Cyber Operation to Attack ISIS Last Year Sparked Heated Debate over Alerting Allies*, Wash. Post (May 9, 2017); *see also* Dustin Volz, *How a Military Cyber Operation to Disrupt Islamic State Spurred a Debate*, Wall Street J. (Jan. 21, 2020); Chris Bing, *Command and Control: A Fight for the Future of Government Hacking*, CyberScoop (Apr. 11, 2018).

73 Hannigan, *supra* note 34, at 32.

74 *Id.* at 31.

75 *Id.*

76 *Id.*

77 Conrad Prince, *On the Offensive: The UK's New Cyber Force*, Royal United Servs. Inst. for Def. and Security Stud. (Nov. 23, 2020) (quoting then def. sec'y Philip Hammond).

78 Osborne, *supra* note 41.

79 *UK Launched Cyber-Attack on Islamic State*, BBC News (Apr. 12, 2018).

80 *Id.*

81 Deborah Haynes, *Into the Grey Zone: The "Offensive Cyber" Used to Confuse Islamic State Militants and Prevent Drone Attacks*, Sky News (Feb. 8, 2021).

82 *See, e.g.*, *Britain Steps Up Cyber Offensive: New £250m Unit to Take on Russia and Terrorists*, Telegraph (Sep. 21, 2018); Deborah Haynes, *Britain to Create 2,000-Strong Cyber Force to Tackle Russian Threat*, Sky News (Sep. 21, 2018).

83 On NCF, *see, e.g.*, Richard Kerbaj, *Female Spy to Net Terrorists as Head of "Cyber-SAS*," The Times (Sep. 8, 2019); Wallace, *supra* note 2.

84 *See, e.g.*, Dan Sabbagh, *UK Unveils National Cyber Force of Hackers to Target Foes Digitally*, The Guardian (Nov. 19, 2020).

85 *See Britain Puts a New Offensive Cyber Force at the Heart of Its Defence*, The Economist (Dec. 1, 2020).

86 Rory Cormac, *The United Kingdom Doubles Down on Covert Operations*, The Mod. War Inst. at West Point (Apr. 2, 2021).

87 *Id.*

88 *Cf.* Gordon Corera, *UK's National Cyber Force Comes Out of the Shadows*, BBC News (Nov. 20, 2020) ("It has been agreed that the foreign secretary and defence secretary will have a role in signing off different types of operations.").

89 Haynes, *supra* note 81.

90 Kerbaj, *supra* note 83.

91 Press Release, Government Communication Headquarters, National Cyber Force Transforms Country's Cyber Capabilities to Protect the UK (Nov. 19, 2020).

92 Tom Houghton, *Boris Johnson Confirms New National Cyber Force Will Be Set Up in North West*, Business Live (Mar. 16, 2021); Martin, *supra* note 34, at 15.

93 It should be noted that GCHQ has express statutory authority to carry out its functions not only in support of defense and foreign policy goals but also, among other things, directly and explicitly "in support of the prevention or detection of serious crime." *See* ISA, *supra* note 61, § 3(2)(c). NSA and USCYBERCOM do not have such a charge, though there are ample pathways for those entities to share with criminal investigators crime-relevant information that they encounter in the course of their missions, as well as pathways for criminal investigative authorities to seek technical assistance. *See* James Baker & Matt Morris, *Defend Forward and the FBI* (Hoover Inst., Aegis Paper Series) (forthcoming 2021).

94 Prince, *supra* note 77.

95 Reports of an operation to take down Russian-sponsored anti-vaccine disinformation, in late 2020, may illustrate this model in action. Lucy Fisher & Chris Smyth, *GCHQ in Cyberwar on Anti-Vaccine Propaganda*, The Times (Nov. 9, 2020).

96 Hannigan, *supra* note 34, at 30.

97 For a proper discussion of "defend forward," *see* other articles in this series, including especially Ashley Deeks, *Defend Forward and Cyber Countermeasures* (Hoover Inst., Aegis Series Paper No. 2004, 2020); Robert Chesney, *The Domestic Legal Framework for US Military Cyber Operations* (Hoover Inst., Aegis Series Paper No. 2003, 2020); Eric Talbot Jensen & Sean Watts, *Due Diligence and the US Defend Forward Cyber Strategy* (Hoover Inst., Aegis Series Paper No. 2006, 2020).

98 Chesney, *supra* note 97.

99 10 U.S.C. § 394 note (2018) (Active Defense Against the Russian Federation, People's Republic of China, Democratic People's Republic of Korea, and Islamic Republic of Iran Attacks in Cyberspace).

100 Hon. Jeremy Wright, Att'y Gen., U.K. Att'y Gen. Off., Speech at Chatham House, Royal Institute of International Affairs: Cyber and International Law in the 21st Century (May 23, 2018).

101 *Id.*

102 *Id.*

103 *Id.*

104 Brian Egan, Legal Adviser, U.S. Dep't of State, Remarks at Berkeley Law School: International Law and Stability in Cyberspace (Nov. 10, 2016) (emphasis added).

105 Robert Chesney, *The Pentagon's General Counsel on the Law of Military Operations in Cyberspace*, Lawfare (Mar. 9, 2020).

106 Ney, *supra* note 71.

107 Jack Goldsmith and Alex Loomis, "*Defend Forward" and Sovereignty* (Hoover Inst., Aegis Series Paper No. 2102, 2021).

108 *See* Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations 17 (Michael N. Schmitt & Liis Vihul eds., 2017) ("A State must not conduct cyber operations that violate the sovereignty of another State.").

109 The list includes France, Austria, the Czech Republic, Finland, Germany, the Netherlands, New Zealand, and others. *See, e.g.*, Jack Kenny, *France, Cyber Operations and Sovereignty: The "Purist" Approach to Sovereignty and Contradictory State Practice*, Lawfare (Mar. 12, 2021).

110 For a full account, *see* Chesney, *supra* note 97.

111 *See supra* note 70 and accompanying text.

112 Wright, *supra* note 100.

113 Ashley S. Deeks, *Intelligence Communities and International Law: A Comparative Approach*, *in* Comparative International Law 259 (Anthea Roberts, Paul B. Stephan, Pierre-Hugues Verdier, and Mila Versteeg eds., Oxford Univ. Press, 2018).

114 *See* Martin, *supra* note 34, at 9 (observing that concerns unleashed in the UK by the disclosures of former NSA employee Edward Snowden "did not provide the ideal backdrop" for announcing that NCSC would be placed within GCHQ, but also noting that the UK public's reaction to those disclosures "was far more muted than it was in the United States").

27 26 25 24 23 22 21 7 6 5 4 3 2 1

The preferred citation for this publication is Robert M. Chesney, *Adapting to the Cyber Domain: Comparing US and UK Institutional, Legal, and Policy Innovations*, Hoover Working Group on National Security, Technology, and Law, Aegis Series Paper No. 2103 (May 25, 2021), available at https://www.lawfareblog.com/adapting-cyber-domain-comparing-us-and-uk-institutional-legal-and-policy-innovations.

About the Author

Jennifer Hancock

ROBERT M. CHESNEY

Robert (Bobby) M. Chesney is a professor at the University of Texas School of Law and director of its Robert S. Strauss Center for International Security and Law. He is a cofounder and contributor to the *Lawfare* blog and writes frequently on topics relating to cybersecurity policy and law.

The Jean Perkins Foundation Working Group on National Security, Technology, and Law

The Jean Perkins Foundation Working Group on National Security, Technology, and Law brings together national and international specialists with broad interdisciplinary expertise to analyze how technology affects national security and national security law and how governments can use that technology to defend themselves, consistent with constitutional values and the rule of law.

The group focuses on a broad range of interests, from surveillance to counterterrorism to the dramatic impact that rapid technological change—digitalization, computerization, miniaturization, and automaticity—are having on national security and national security law. Topics include cybersecurity, the rise of drones and autonomous weapons systems, and the need for—and dangers of—state surveillance. The group's output will also be published on the *Lawfare* blog, which covers the merits of the underlying legal and policy debates of actions taken or contemplated to protect the nation and the nation's laws and legal institutions.

Jack Goldsmith is the chair of the National Security, Technology, and Law Working Group.

For more information about this Hoover Institution Working Group, visit us online at http://www.hoover.org/research-teams /national-security-technology-law-working-group.

Hoover Institution, Stanford University
434 Galvez Mall
Stanford, CA 94305-6003
650-723-1754

Hoover Institution in Washington
The Johnson Center
1399 New York Avenue NW, Suite 500
Washington, DC 20005
202-760-3200

HOOVER INSTITUTION