Intelligence in the Cyber Era: Evolution or Revolution?

David V. Gioe, Assistant Professor of History and History Fellow, Army Cyber Institute, United States Military Academy at West Point.
Michael S. Goodman, Professor in Intelligence and International Affairs and Head of Department of War Studies, King's College London.
Tim Stevens, Senior Lecturer in Global Security, Department of War Studies, King's College London.

Abstract

The hyper-connectivity of global information networks in contemporary societies is one of the greatest technological developments in human history. It has occasioned much reflection and marvel, yet also hand-wringing over the societal disruption, as well as the proper scope of intelligence and security agencies in harnessing these developments in a game of cat-and-mouse with evermore-sophisticated state and non-state adversaries. History suggests that intelligence services have adapted to past technological innovations in productive fashion, but how have their responses to 'cyber' developed, and why? Given its centrality to understanding what intelligence agencies do, the following account situates Anglo-American cyber developments within the traditional intelligence cycle and considers how contemporary information technologies and processes affect intelligence collection and analysis. We also address the issue of offensive cyber operations, which are increasingly treated as an intelligence function. Intelligence occupies a central role as a lever of state power, and is required to be a source of competence and capability, a driver of change, and responsive to shifting political calculations. Yet has the cyber age fundamentally transformed intelligence bureaucracies and their operations in the way that it has surely done for everyday life? We conclude that the cyber era has occasioned a technological revolution, but not an intelligence revolution. To exploit the cyber revolution to gain decision advantage, intelligence communities must integrate cyber into traditional collection and analysis efforts, but they must balance application of these technologies with societal transparency and political oversight.

INTRODUCTION

The emergence of global hyper-connectivity through computer networks has occasioned much marvel, reflection, and commentary on its implications for everything from 'just-in-time' supply chain management to the Internet of Things. These developments are also consequential in national security and intelligence. What must objectively be seen as technological progress has also sparked

debates that would have been unimaginable half a century ago, and in fields far beyond computer and political sciences. The desire to protect informational assets from theft, subversion and degradation, and questions about how to exploit networked computing for strategic gain, have spurred remarkable developments in intelligence collection, policy, doctrine, law, strategy, and even ethical norms. There are active debates about how cyber considerations affect each field touched by them, and it seems that there remain more unsettled than settled questions about cyber power as a lever of statecraft in the twenty-first century.

Along the way, multiple claims have been made for the transformational impact of 'cyber' and its peculiar challenges as to how practitioners approach traditional conceptions of security and the consequent effects on national power and international order. Many perceive radical transformations stemming from an 'information revolution', sometimes leading to alarmism, hyperbole, and demands for new forms of security politics and practice. Such concerns often find their expression as cyber versions of momentous twentieth-century events, such as the possibility of a 'cyber Pearl Harbor'[1] or a 'cyber Cuban Missile Crisis'.[2] Others prefer not to throw out the historical baby with the technological bathwater and seek to apply traditional analytical frameworks to contemporary problems of cyber security and insecurity.[3]

It is, of course, difficult not to appreciate that networked information technologies have changed the world in multiple ways. The manner in which digital interactions have altered everyday life and engendered the extraordinary would seem incomprehensible to people only a few decades ago. Scholars, regulators, practitioners, and business executives are therefore reaching for any available tool or service that enables them to understand this complex environment and facilitate appropriate action in and through it.

One common gambit in the non-technical literature is to construct threat-based typologies that facilitate directed research and response.[4] Categorisation of cyber threats by functional effect, for instance, leads to a tripartite distinction between disruption, espionage and degradation.[5] Based on the type of threat actor involved, we encounter cyber war and cyber warfare, cyber crime, cyber terrorism, hacktivism and cyber espionage or intelligence.[6] The empirical evidence suggests significant fluidity between and across these diverse groups of actors, but these categories retain utility in distinguishing agendas when discussing cyber threats and planning countermeasures. Of course, executive responsibility and legal lanes of the road in response to cyber threats are often exacerbated by the fluidity of threat typologies and competing definitions. Discord, especially in the area of cyber law, can lead to decision paralysis. The on-again, off-again decision of whether to separate United States Cyber Command from the American National Security Agency (NSA) is suggestive of this structural governance challenge.[7]

The focus on actors reveals something else useful as well. In the security and strategic studies literature, far more attention has been granted to issues of cyber war and warfare than other cybersecurity phenomena. In the case of cyber terrorism, this is due to the paucity of examples upon which to found well-rounded investigations. Cyber crime has its own burgeoning literature in the fields of policing and criminology and, like hacktivism, tends to occur below the level of the state and war. This is not the case for intelligence, however, which is driven by national purposes and interests. It is therefore curious that cyber espionage – in its state, rather than commercial, manifestation – and cyber intelligence have received far less explicit attention than might have been expected.[8] In particular, even as there is no question that cyber technologies are novel, as are many of the intelligence opportunities presented by them, how does this compare to the ways in which intelligence communities have responded and adapted to previous phases of

technological disruption? This question motivates the present enquiry, in which we identify issues of continuity and change in intelligence priorities and rationale. If we accept that change is endemic in intelligence responses to shifting technological contexts, what is the nature and impact of this change today? What has altered and what stays the same? In short, has the cyber era ushered in an intelligence revolution, and how – and how successfully – has the Anglo-American world grappled with this development?

REVOLUTION: BRIEF LITERATURE REVIEW, CONCEPTS, APPLICATION

A core element of this article concerns the concept of revolution – as distinguishable from evolution – in the adaption to, and adoption of, technology in Anglo-American intelligence communities. As it relates specifically to intelligence, 'revolution' is an oft-used but rarely defined term. In the field of intelligence studies, the idea of a 'revolution' has been limited to a tangent of the broader strategic debate that emerged in the early 1990s on the so-called 'Revolution in Military Affairs' (RMA). This was the change affecting advanced militaries whereby technology allowed different elements to be brought together into a single information-based system, at times also called 'net-centric warfare'.[9] The envisioned benefits were clear, allowing sophisticated militaries to enhance their capabilities and efficiency in harnessing information technology to widen the force capability gap between the technological haves and have-nots on the battlefield.[10]

One dimension of the RMA was information and intelligence; thus, a brief debate emerged about whether the RMA was accompanied by an identifiable 'revolution in intelligence affairs', as was argued by Eric Denece.[11] Or, should such a change have occurred after 9/11? As one RAND report suggested, 'a "revolution in intelligence affairs" is needed to prepare the [U.S.] Intelligence Community to meet its future challenges'.[12] The conclusion from this brief foray into intelligence

revolutions was inconclusive and in any case largely focused on intelligence support to military operations in particular as in John Ferris' study.[13] Broader theoretical applications beyond warfighter support were underdeveloped despite notable efforts.

The phrase 'revolution' has been applied scattershot elsewhere in intelligence studies, from the transitional democratic reforms in Eastern Europe and its surveillance heritage post-1989 to the rise of al-Qaeda and its effect on intelligence operations.[14] The missing element to these discussions is a sense of what a 'revolution' in intelligence terms might comprise, especially if occasioned by technological leaps. Is it possible to observe that an intelligence revolution is underway before it is finished and retrospectively analyse what changed? With the RMA it was clear that technology influenced change in military doctrine and business practices, but this did not equate to a broader change in intelligence support to military operations *per se*; rather, its application in one particular sphere had provided the catalyst to military revolution. A decade later, the attacks on 9/11 required a change in intelligence structure and focus, but not a wholesale transformation in core processes or *raison d'etre*.

In the cyber literature, 'revolution' is encountered more often, including in the recent work of political scientist Lucas Kello. In his research on cyber weapons, Kello developed a conceptual framework to analyse technical revolutions in international relations, but his focus is on the nature of the weapons and their application in international order instead of narrower intelligence dimensions. He identified three distinct 'orders' of cyber revolution, including systemic disruption, systemic revision, and systems change, exploring their theoretical dimensions. In Kello's estimation, we are in an age of cyber revolution as evidenced by the rapid expansion of cyberspace into nearly every facet of human activity and the disruptive rebalancing of actors and their activities in the international order, leading him to conclude, 'the distinguishing feature of security

affairs in the current epoch is not the existence of a revolution condition but the prospect that it may never end'.[15]

We endorse Kello's finding of a revolution in cyber, but what might an *intelligence* revolution in the cyber era look like? Three of Kello's criterion may be usefully applied to a study of intelligence in this context: first, an intelligence revolution would involve a rapid change to the nature and practice of intelligence work; second, the nature of the change would be systemically disruptive; and third, that a reordering of global intelligence capabilities of states would result. As the balance of this article will explore, there has not been a rapid modification of the nature and practice of intelligence work; the technological impact has been transformative over time, but not necessarily disruptive in the immediate sense; and although there has been a rebalancing of intelligence capability across state and nonstate actors thanks to cyber activities, the intelligence powers widely considered to be in the first tier have not been supplanted by other actors solely on the basis of their exploitation of the cyber revolution. We therefore advance the notion of 'evolution' in this article; in other words, the changes ushered in by the cyber era and their impact on intelligence work are more appropriately the latest incarnation of technological advances that have affected the Anglo-American intelligence communities. Further, changes that might be revolutionary in a technological sense are not necessarily so in a purely intelligence sense. These changes are slower-paced and iterative, and the effect is therefore more appropriately characterised as evolutionary rather than revolutionary.

The nature of the practice of intelligence endures. The most adept intelligence communities will learn to master the cyber domain and use it to gain decision advantage for their political masters, just as they have done with the putatively revolutionary technologies the past. In an analogous context to the RMA, those, on the other hand, who fail to incorporate cyber

considerations into their traditional business practices will find the delta between their efforts and the more adaptive communities ever-widening, thus suggesting a possible substantial decrease for some states in this critical area of state power in the international system. Whether their cyber adaptation success or failure can fundamentally reorder the intelligence prowess of global competitors remains to be seen. Our argument unfolds in two main approaches: first, we present an historical overview of previous technological revolutions, considering how the Anglo-American and also Soviet/Russian intelligence communities integrated what were, at the time, ground-breaking changes to their working environment and purpose; second, we take the more specific changes introduced in the cyber era and considers in what applications they may be novel to the work of advanced intelligence communities generally.

TECHNOLOGICAL CHANGE AND THE TRANSFORMATION OF INTELLIGENCE

Technological change matters because it forms the backdrop to – and is a key driver of – the evolution of intelligence practice. In fact, it is likely that no development is as significant as technological change in terms of what adoption and implementation might mean for international security beyond intelligence bureaucracies. Michael Warner emphasises this relationship: 'technological change shapes and re-shapes both the threats to the state as well as the opportunities available to it in the international arena, and thus it plays a role in determining the targets of intelligence *and* the means that intelligence employs'.[16] To explore this construction further, we build upon David Omand's proposition regarding the four 'technological revolutions in intelligence'.[17] Each is identified with major technological innovations of the twentieth-century: exploitation of the electromagnetic spectrum; programmable computers; electro-optics; and the Internet. We have added a fifth – aerial and orbital reconnaissance – between electromagnetic

exploitation and programmable computers, to account for the proliferation of aerial and orbital information technologies after World War II. We consider each in turn with reference to specific technological developments and their impact on intelligence practice and priorities, underscoring the political significance of key developments at each stage.

Electromagnetic Exploitation

The first putative revolution in intelligence was occasioned by the discovery by Guglielmo Marconi and Heinrich Hertz of radio waves and electromagnetic radiation in the late nineteenth century. Marconi's construction of a system of wireless transmission and reception of radio signals was game-changing.[18] He was not the first to demonstrate these capabilities but he was significant in showing they could be deployed practically and on a cost-efficient basis. His initial experiments were successful in transmitting and receiving a signal over a distance of a few miles, but Marconi was alert to the need for sustained funding to increase the effective range of this technology. In 1896, he travelled from Italy to London to seek patronage. With this secured, he subsequently transmitted a Morse signal nearly ten miles, attracting public – and political – attention. In 1901, he claimed to have sent a message 3,000 miles across the Atlantic. The British government was quick to identify the military and intelligence potential of Marconi's work.[19] Before wired communications became the norm, with arrays of wires installed on poles across Britain and planted on the Atlantic seabed, communications intelligence (COMINT) was gleaned from the interception of letters, responsibility for which lay with the Post Office.[20] From the mid-nineteenth century onwards, Britain also practised signals intelligence (SIGINT), the interception of wired communications and codebreaking, yet these two activities were placed in different organisations that seldom co-ordinated their activities,[21] suggesting early adoption was marred by *ad hoc*

governmental implementation. Marconi's work and World War I broke these silos, revealing that the combination of capability and necessity would drive both international politico-military developments as well as *sub rosa* intelligence advancements.

Radio researchers working for Marconi at the start of the war discovered that the 'ether' was rich in radio messages.[22] This came as a surprise to the War Office and Admiralty,[23] but they did not compound the oversight with foot-dragging. In fact, within just a few months, British naval intelligence reorganised and, equipped with captured German codebooks, began to intercept, decipher and translate messages. Room 40, as the naval code-breaking centre in London was known, was a resounding success. A wireless interception station, the first of its kind, was set up at Scarborough to monitor and direction-find the communications of the German *Hochseeflotte*. The Army followed suit with MI1B, its SIGINT outfit that processed intercepted signals from the Western Front. In addition, a separate diplomatic codebreaking unit was created on behalf of the Foreign Office. There was limited interaction between these units until the latter part of the war, as each had its own discrete mission, but they were able to achieve some remarkable successes.[24]

Throughout the war, British intelligence kept pace with developments in wireless communication, suggesting that British intelligence could be considered an early adopter of technology in the proto-cyber age, and indeed would be rewarded for such prescience in the next war. Ferris calls this period the beginning of 'modern intelligence', given the scientific advances in transmission and breaking of wireless codes. For the intelligence agencies, 'extraordinary efforts' were required to overcome technical hurdles, efforts that would prove invaluable when Europe once again found itself at war in 1939.[25]

Between the wars, scientific advances continued apace, and government, academia and industry collaborated in loose fashion to maintain British advantage. The creation in 1919 of the

Government Code and Cypher School (GC&CS) was a positive step in uniting experience and expertise in the services and beyond. The British government provided GC&CS with significant funding, and through the 1920s and 1930s it was regularly able to read the encrypted communications of Japan, the United States and Italy, and, to a lesser extent, those of France and the Soviet Union. By 1939, many of these codes had been upgraded and access was lost. U.S. and French messages could still be read, but in the former case only until Churchill cautioned Roosevelt about flaws in the U.S. diplomatic cipher system.[26]

In September 1939, Britain declared war on Nazi Germany. Many of its World War I codebreakers were still involved in the field but were under no illusions that the earlier widespread access to enemy codes would be repeated. Admiral Sir William James, Deputy Chief of Naval Staff and a former member of the Admiralty's secretive 'Room 40', recorded, 'I do not believe we will ever again enjoy all the advantages of the 1914-1918 war, because people today are wiser about wireless'.[27] The impact was obvious to all involved: the known weaknesses of wireless transmissions and proven successes in interception ensured that once hostilities began, wireless radio silence would be observed. Here, GC&CS' inter-war work was essential, not only in breaking foreign codes but also in providing means of secure communication.

The British government, however, was not the only one seeking more secure communications through adoption of emerging technologies. Berlin also wished to harness technological developments for its own communications security and adopted an upgraded version of the hitherto commercially available Enigma cipher system, which offered mind-boggling combinations to secure wireless traffic. However, this technological marvel generated overconfidence. By 1939, not only was Germany's overwhelming reliance on the Enigma cipher system known, but extensive effort had already begun to break it. The impetus came from Poland,

but it would be intensive British work that cracked the system and provided what Ferris calls a 'cryptological revolution'.[28] British success was not only technical, but also resided in how decrypted Enigma traffic was analysed and used to further British strategic goals. The second half of the war saw this work increase in importance and we can see in this period the emergence of another transformational technology: programmable computers.

Programmable Computers

Alan Turing, along with lesser-known figures like Konrad Zuse and Alonso Church, is one of the key progenitors of computer science. A Cambridge mathematics graduate, he specialised in computational theory, developing foundational ideas in hypothetical computing machines that shaped how we conceptualise and build computers today. Between 1936-1938, Turing worked at Princeton on his PhD, part of which dealt with cryptology. He later returned to Cambridge and was recruited to GC&CS, where he worked on cryptanalysis of Enigma. Turing was part of the team that cracked Enigma codes and constructing the bombe, a large and sophisticated electromechanical machine that could replicate the settings on an Enigma device in order to decipher encoded messages.[29]

This was not Turing's only wartime achievement, but his chief legacy to intelligence lies in his demonstrating how programmable machines could work in a logical rather than mechanical sense. His pre-war work on hypothetical computing combined with his wartime practical applications showed how some processes of intelligence analysis could be automated. That Turing and his colleagues were given relatively lavish funding and nearly free rein to experiment in a time of national crisis, with personal support from Prime Minister Winston Churchill, is a credit to the

wartime government and also a petri dish for what was to bloom at the post-war successor to GC&CS and Bletchley Park, the Government Communications Headquarters (GCHQ).

Aerial and Orbital Reconnaissance

Parallel post-war advances in valve technology, for example that of the radar, and later developments in transistors and solid-state electronics, allowed for electronic devices small enough to be incorporated in satellites and propelled into orbit. Satellite technology would change fundamentally the pattern of intelligence investment in the United States and the USSR[30], although while such remarkable collection types provided a new stream of reliable intelligence, it was fused into all-source analysis and provided to policymakers in the ways that had been done before they came online. Still, in many respects, the Cold War was characterised by technological competition enabled by and fought through technological advances. In the military sphere, jet engines, stealth technology and thermonuclear weapons altered the character of warfare. The means of governmental communication also evolved rapidly, with faster and more secure methods developed amongst the major powers, allied to novel means by which communications could be intercepted and exploited for intelligence value.[31]

For intelligence communities, the changes were no less profound. Advances in aerial and orbital reconnaissance were staggering, in terms of platforms, cameras and sensors, the wavelengths captured and, eventually, the ability to download digital products directly to workstations. Lockheed's U-2 and SR-71 reconnaissance aircraft, and any number of satellite platforms such as Corona, enabled photographic evidence and, later, infrared and radar images and signals to be obtained from previously impenetrable areas, often considered 'denied areas' for traditional human intelligence (HUMINT) collection efforts. After a series of collection and

recovery developments, these technical marvels were available to analysts in near real time. Critically, analysts learned to incorporate such special collection into their traditional intelligence cycle of requirement tasking, collection, processing, and analysis with dramatic international political ramifications. For instance, advances in camera resolution and the ability to 'see' through clouds would prove useful when married with the HUMINT reporting of Soviet military intelligence (GRU) Colonel Oleg Penkovsky which revealed the capabilities and employment doctrine of Soviet nuclear-capable missiles in Cuba.[32] This all-source analysis enabled the United States Ambassador to the United Nations, Adlai Stevenson, to present incontrovertible evidence of Soviet deeds to the United Nations in 1962 and helped the John F. Kennedy administration defuse the Cuban Missile Crisis and, arguably, avoid World War III.[33]

The gap between traditional human approaches to intelligence and sophisticated technical means grew, but also routinely converged symbiotically in certain complex operations, the forebears of technological development enabling other collection methods that have evolved in contemporary terms like 'cyber-enabled HUMINT' or the converse 'HUMINT-enabled cyber operations' such as the Stuxnet attack on Iran's nuclear programme.[34] Intelligence successes often fused the two collection typologies, such as the deployment of miniaturised cameras and bugging equipment by human assets. In Britain, scientific and technical intelligence had its own committee from the end of World War II and dedicated personnel working on it.[35] Similarly, the Central Intelligence Agency (CIA), created in 1947, was quick to recognise the importance of science and technology to intelligence work, and in 1949 founded the Office of Scientific Intelligence.[36] Scientific intelligence, then, was not only about novel means of gathering intelligence, but also enabled and provided for detailed analysis of technical subjects.[37] To this end, the intelligence agencies often worked closely with private contractors to develop these capabilities, particularly

in the United States, a historical legacy with far-reaching contemporary relevance. Indeed, that in 2015 CIA established an entirely new Directorate, a first in decades, of Digital Innovation (DDI)[38] connotes how seriously the U.S. intelligence community assesses the impact of cyber developments on its core mission.

Through the radical distribution of semi-automated data-gathering technologies and computer-assisted analysis, intelligence agencies leveraged the legacy of Turing and others to create capabilities that promised 'total oversight, exacting standards of control, and technical-rational solutions to a myriad of complex problems'.[39] Informed by and driving managerial processes like that of Robert McNamara's systems analysis, intelligence practitioners shared this outlook with the U.S. military.[40] As the United States discovered in Vietnam, this approach, infused by mid-century cybernetic dreams of frictionless command-and-control, often encountered resistance during the dirty reality of war.[41]

In the world of intelligence, however, a great deal of actionable intelligence was generated through harnessing scientific sources and methods. In this respect, technological and organisational innovation by the United States in general helped stabilise the superpowers' nuclear standoff,[42] but also with notable exceptions when attempts to harness scientific breakthroughs went awry, such as the shooting down of American U-2 pilot Francis Gary Powers over Soviet airspace on 1 May 1960. These events often had significant international political consequences. The Powers incident, for example, prompted the cancellation of a planned superpower summit in Paris, which aimed to resolve lingering questions about a divided Germany and establish missile test bans.[43]

Electro-optics

The fourth technological 'revolution' that impacted intelligence concerns the mastery of the physics of light. This includes the laser for rapid reading and writing of data at speed, and the manufacture of solid-state devices that, following Moore's Law, has meant year-on-year increases in computing power.[44] It also includes the creation of fibre-optic cables for transmitting vast volumes of data at the speed of light in that medium. Omand identifies these developments with charismatic theoretical physicist Richard Feynman, who cut his teeth on the wartime Manhattan Project, where he worked in the theoretical physics division.[45] After the war, Feynman moved between various leading U.S. universities, studying an array of physics problems. He is probably best known for his research into quantum electrodynamics, for which he received a Nobel Prize in 1965.[46] A field of particle physics, this explores the manner in which light and matter interact, essential for the technologies underpinning solid-state devices, rapid computer processing and memory, and fibre optics, all of which transformed global communications and thus communications intelligence.

The work of Feynman and many others ushered in the utilization of digitised information by intelligence agencies. This was the start of the digital age, the shift from typewriters to word processors, from information stored on paper to electronic storage at scale. Computers had begun to communicate with each other in the 1960s with the Advanced Research Projects Agency Network (ARPANET), but it was not until the 1970s that they started to become commonplace in government.[47] This led to intelligence agencies targeting those with access to repositories of information (data at rest).[48] In a sense, this was not a wholly novel enterprise: history is replete with spies, defectors, and whistleblowers with access to registries and archives. Infamous Soviet agent Kim Philby, for instance, spent part of the war working in the UK's Secret Intelligence

Service (SIS, also known as MI6) registry in the evening and it is difficult to know quite what he might have accessed during that time.[49] Decades later, Soviet KGB officer Vasili Mitrokhin defected to British intelligence, bringing reams of valuable material with him. Mitrokhin was the KGB's archivist and although his material was historical in nature, nonetheless it revealed the identities of many former Soviet agents in the West and beyond. Mitrokhin's work with Christopher Andrew shed much-needed light on the missing dimension of intelligence as a critical component of international history.[50]

Less well known are two American examples. In 1960, two NSA cryptologists, William Martin and Bernon Mitchell, defected to the Soviet Union. Supposedly upset at NSA's collection activities and the lack of Congressional oversight, they slipped over the border to Mexico, travelled to Cuba, and from there sailed to the Soviet Union. Months later, they appeared in a joint news conference in Moscow, declared their allegiance to the Soviet Union, condemned the activities of the NSA, and requested asylum. Neither would return alive to the United States. It is not known whether they were targeted by the Russians, or if they had simply developed strong communist convictions. Regardless, their betrayal undoubtedly revealed significant information about the inner workings of the NSA.[51] Later, Perry Fellwock, also known as Winslow Peck, became the NSA's first public mass leaker. In the early 1970s, disenchanted with the NSA's global SIGINT programme, ECHELON, he revealed details in *Ramparts* magazine, which ended up on the front page of *The New York Times*. Not only did Fellwock reveal a startling amount of operational detail, including the types of security badge worn at NSA headquarters, but he also declared that the Americans were reading Soviet codes.[52]

This was not entirely true, but the point is that the technological developments in computing and secure communications saw an increase in the specific targeting of those working

in electronic areas on both sides of the superpower standoff.[53] One example concerns Markus Hess, a German citizen who was recruited by the KGB in the 1980s to hack into U.S. military systems. Hess was based at the University of Bremen but was able to access the Tymnet international gateway, through which a range of other computer networks could be accessed. Before his activities were uncovered, he accessed two significant networks: the ARPANET civilian system, used in part by the Department of Defense, and its military equivalent, Military Network (MILNET). In total, Hess hacked into 450 classified military computers. The case is illustrative for a number of reasons: the deliberate targeting of sensitive U.S. communications; the ability of an individual overseas to obtain wide access into U.S. classified systems; and the manner in which national governments had to cooperate to disrupt the operation. Hess was eventually caught, found guilty of espionage, and sentenced in a West German court to a short prison sentence, largely because laws involving computer crimes were in their infancy and governments had not yet begun to pass suitable laws to govern the looming cyber age.[54]

Another example of skilful Soviet intelligence adoption of technological developments is the Gunman Project. In the mid 1980s, the United States Embassy in Moscow ordered a new set of electronic typewriters. Unknown to the Americans, the typewriters were intercepted in transit by Soviet intelligence. Operatives installed a simple yet clever device on the machines that was both wireless and remotely controlled. Using antennae hidden in the walls of the Embassy, the bugs could transmit anything typed on the machines to listening posts located nearby. Over a two-year period, the Soviets were able to read anything typed on sixteen such compromised machines as the keystrokes were captured and transmitted before being encrypted, thus rendering ineffectual the best efforts of American codemakers. How U.S. intelligence discovered the operation has been excised from the official NSA account, but once it became known, the Americans raced to replace

all the electronic equipment in the Embassy.[55] Such successes were paralleled in the Soviet Union and it has been claimed that by the early 1980s, the Soviets spent over 2% of their intelligence budget on such efforts.[56] These operations would be referred to as 'supply chain threats' in contemporary vernacular but form a piece with enhanced attempts to target information and information technologies in an increasingly transnational global environment. Indeed, the Soviets, and subsequently the Russians, would show as keen an interest as any other country in harnessing cyber as a lever of state power.

The Internet

The early networks outlined above underwent significant and irreversible transformation at the beginning of the 1990s. The ARPANET and MILNET networks compromised by Hess were predominantly military constructions, with an important admixture of academic, and increasingly corporate, nodes. Utilising packet-switching technology developed independently in the United States and UK, these networks provided the foundations for the modern Internet that developed during the 1980s.[57] It was not until 1991, however, that widespread public access to the Internet was practicable, facilitated by the release of the World Wide Web and the first web browser.[58]

The legacy of this work is phenomenal and, whilst important social and political effects are apparent, its long-term implications have yet to be discerned. Its implications for intelligence, however, can already be considered profound. An important conceptual transition occurred during this period. The preceding technological developments, in the exploitation of the electromagnetic spectrum, computing, reconnaissance, and the extension and intensification of global communications networks, reached their apotheosis in the creation of the Internet. For many, this

heralded a fundamental transition from industrial modernity to a new post-industrial, 'information society'.[59]

Driving and reinforcing this change was a cognitive shift towards viewing society through an informational lens, in which all manner of interactions and artefacts were rethought in informational terms. The U.S. military reformulated the instruments of national power as diplomatic, informational, military and economic (DIME) and the role of information and information technologies as strategic assets and vulnerabilities came increasingly to the fore.[60] As is common with technological disruptions, the language of revolution was never far away. Often wrapped up in the loaded – and notoriously hard to define – term 'cyber', these developments attracted excited concern, not least from General Michael Hayden, the former director of both CIA and NSA, who asserted that 'this cyber thing is probably the most disruptive event in human history since the European discovery of the Western hemisphere'.[61] He is probably correct, but 'everything has changed' narratives tend to overlook empirical detail and important political and practical effects.[62]

This is as true of intelligence as any other field. Intelligence agencies are now required to operate in a global information environment in which national borders are porous and frequently irrelevant, and in which diverse state and non-state actors play important roles. They also operate across computer networks that blur conventional distinctions between public and private. These dynamics have required intelligence agencies to rethink their traditional roles and forge new and unfamiliar relationships with a variety of state and non-state partners.[63] The lines are also blurring between the worlds of digital and semantic information, as the Russian 'cyber-enabled information operations' relating to the 2016 U.S. presidential election demonstrate.[64]

Intelligence agencies are also subject to unprecedented public scrutiny. The fallout from the Snowden disclosures showed that surveillance ('watching from above') practices conducted by state intelligence agencies could on occasion be matched by public sousveillance ('watching from below') and activism.[65] This has heightened awareness about intelligence transparency, accountability and oversight, and led to significant changes in how intelligence agencies interact with the public sphere.[66] In the United States and UK, for instance, public disquiet and debate led to significant revisions of the legal and constitutional footings of SIGINT agencies and their operations.[67] Such key developments in governmental attempts to manage change, especially rapid technological change, are benchmarks that are hard to overstate.

These are all developments of public record, but less attention has been granted to the actual work of intelligence agencies under these conditions. As previous sections relate, intelligence has adapted to past technological innovations in productive fashion. How do their responses to 'cyber' compare? Given its centrality to understanding what it is that intelligence agencies do and why, the following account situates cyber within the intelligence cycle. This is the standard transatlantic approach to intelligence activity. In its simplest form it describes the cyclical and iterative process in which the intelligence community interacts with decision makers to prioritise requirements, collect, analyse and interpret intelligence, and then disseminate it to those whose responsibility it is to act upon it.[68] The following sections consider the different stages of the intelligence cycle: how intelligence collection, processing and analysis are affected by contemporary information technologies and processes. We also address the issue of offensive cyber operations, which are increasingly treated as a function of intelligence and its handmaiden, covert action.

INTELLIGENCE COLLECTION

This section considers the impact of the cyber era on arguably the most controversial and fraught stage of the intelligence cycle, as described above. Intelligence collection and the cyber domain can be considered in two related ways: the use of cyber as a collection technique, either on its own or in co-ordination with other traditional collection techniques as noted in the HUMINT-enabled Stuxnet example above; or, as the target of collection efforts itself. The great advantage of using digital means to collect intelligence is the issue of distance and, secondarily, plausible deniability if caught, a function of the challenge of 'attribution'. One former director of the CIA's Clandestine Information Technology Office noted that 'clandestine technical collection no longer requires physical proximity to the target. U.S. information systems can be remotely targeted and their secrets collected and exfiltrated to any part of the world'.[69] This highlights the fact that vulnerability is the converse of opportunity, particularly for intensively networked countries like the United States, but also brings to the fore wider issues about access. Historically, huge efforts were invested in targeting appropriate individuals for recruitment, not only because of potential susceptibilities improving the likelihood of recruitment, but because of the intended asset's access to whatever intelligence was being sought.

This situation has changed significantly.[70] The mass theft of data from the United States Office of Personnel Management (OPM) disclosed in 2015 is an intelligence breach of the highest order.[71] The FBI estimates that records of nearly 22 million past and current U.S. federal employees may have been compromised, including much of the intelligence community workforce. This includes Personally Identifiable Information (PII) such as names, addresses and bank accounts that might be used for identity cloning or theft, and records of vetting enquiries for people with security clearances that could identify undercover operatives abroad or provide

possible leverage for blackmail and other purposes. Indeed, it has been alleged but not proven that while CIA employees generally will not have been affected by the hack given that its personnel files were not stored with OPM, by extension anyone known to have been working overseas and not included in OPM files must be a CIA officer.[72] Furthermore, the incident was not an isolated one: the same system was attacked the year before, as was a company providing healthcare insurance to government employees and two companies supplying background checking services.[73] The breach was linked to ongoing cyber infiltrations by China, which thereby emphasised U.S. vulnerability whilst signalling Chinese resolve and capability against the backdrop of deteriorating U.S.-China relations.[74] It is all but impossible to conceive of such an operation by a strategic adversary before the advent of networked digital communications, which provide state and nonstate rivals with new ways of accessing rich data sources and new opportunities for strategic leverage.

This incident raises questions about the volume of material that can be gathered through cyber means. We are in a period of bulk interception and acquisition and 'big data', but arguably this is not without historical precedent. World War II efforts at Bletchley Park were a vast undertaking, particularly given the technology then available. It is estimated that in 1941, an average of 39,000 Enigma reports were deciphered each month, rising to 90,000 in the latter stages of the war.[75] One historian has estimated that in total several million items were intercepted, decrypted and translated over the six years of the war.[76] Another example is an audacious Anglo-American effort at the height of the Cold War. In 1954, realising that telephone wires carried Soviet military communications beneath the streets of Berlin, the Anglo-American partners began complex engineering works to excavate 3000 tonnes of earth. The cables were a mere 50 centimetres below street level and all the groundworks had to be undertaken without arousing

suspicion. The resulting tunnelling and intelligence operation lasted for just under a year. Despite its existence being betrayed from the outset by George Blake, a Soviet penetration of SIS, it provided baseline intelligence via approximately half a million intercepted telephone calls.[77]

Another aspect of data extraction is its new-found portability via digital means. Aldrich Ames, the KGB mole inside the CIA, offered an early example of this when he copied thousands of pages of documents onto floppy disks.[78] By contrast, Edward Snowden is reputed to have purloined over a million U.S. documents, plus 58,000 British and 15,000 Australian.[79] Snowden also highlighted the role a single individual can play in procuring digital intelligence. As David Anderson, then the British government's Independent Reviewer of Terrorism Legislation, concluded that Snowden's actions 'demonstrate the impact that can be inflicted by a single well-placed individual with wide network access'[80], thus expanding conceptions of the types of dangers posed by insider threats beyond terrorism.

The 'insider threat' is a well-recognised aspect of organisational cybersecurity, which means that intelligence institutions will continue to look inwards as much as they do outwards. Another example of the failure of internal security is provided by former U.S. soldier Chelsea Manning, who provided 750,000 U.S. military and diplomatic documents to WikiLeaks,[81] an organization characterized by former CIA Director Mike Pompeo as a 'non-state hostile intelligence service'.[82] An interesting similarity between Ames and Snowden is that despite possessing significant electronic archives, each passed on confidential data by means of physical storage devices. In contrast, Manning uploaded data remotely and had no direct physical contact with the recipients. Intelligence agencies must cope with various forms of illicit communications emanating from within, as part of their wider operational security mission. Like all institutions

coping with multiplying vectors connecting their insides with the outside, intelligence agencies are finding they are also 'leaky containers'.[83]

There are historical precedents of individuals providing high-level reliable intelligence, often over a period of years, but the volume and portability of material then pale beside contemporary challenges. At the same time, statistics and storage sizes do not tell the whole story. It is more useful to consider quality rather than quantity of information and assess the impact of individual disclosures. The OPM hack has led to management resignations and intense Congressional concern, but its longer-term effects are difficult to determine. Indeed, it would be facile to conclude that a future penetration of the U.S. intelligence community was recruited solely because their PII was exfiltrated by the Chinese. Snowden's disclosures, however, had an immediate and tangible effect: British intelligence opted to relocate a number of important agents from Russia and China as a precautionary measure,[84] thus hampering the intelligence collection operations of presumably valuable agents. Moreover, the demonstrated inability of the U.S. intelligence community to keep its most precious secrets has jeopardized future intelligence collection.[85]

How Snowden otherwise affected the work of the intelligence agencies is open to debate and often resolves to pre-established notions about the legitimate scope of SIGINT and surveillance. Arguably, there are many historical examples of individuals providing less intelligence than Snowden or Manning but with greater effect, particularly if they were specifically tasked and agreed to remain in place, thus available to service future requirements. In short, quantity is less important than quality and, whilst greater collection efforts are enabled by contemporary information technologies, it is potentially harder to tailor collection to specific requirements. If the NSA's unofficial mantra is 'Collect It All', there may be diminishing returns

on investment in doing so. At present, there is no linear causality between volume of data and actionable intelligence evident to external researchers, as discussed further below, although analytical applications involving Artificial Intelligence (AI) may challenge this status quo.

For intelligence collection, then, cyber has ushered in a new era for intelligence tasking, access, and process, but with significant attendant counter-intelligence threats. Access is important, as is the ability to penetrate a target without leaving obvious traces behind. External espionage and insider threats present new challenges but these are essentially novel versions of established, if problematic, practices. The quantity, breadth, depth and range of sources of information that can be accessed are unparalleled, and the means of collection are different, but the underlying philosophy and reasons for collection have not altered. And, as has been shown, the integration of technological development into traditional intelligence practices can have significant international political effects.

INTELLIGENCE PROCESSING AND ANALYSIS

Increased data collection capabilities have had demonstrable effects on the character of intelligence analysis. The importance of separating signal from noise has never been greater, as SIGINT volumes expand and sources diversify. These data flows constitute valuable resources for intelligence agencies, but deriving operational advantage demands new storage, processing, dissemination and analytical requirements. Storage needs can be met in the short term by building new data centres and computational processing power is guaranteed over a similar period by high-performance computing.[86] The real challenge is in structuring, processing and analysing massive data sets to provide meaningful intelligence that meets tasking requirements and the needs of decision-makers. Since the mid-Cold War, the Anglo-American intelligence community has

pursued machine learning (ML) and it is increasingly accepted that, if effectively harnessed, artificial intelligence will advance the state of the art in intelligence analysis.[87] In mid-2018, Robert Cardillo, director of the American National Geospatial-Intelligence Agency (NGA), stated that his agency will incorporate facets of AI, augmentation and automation (AAA) broadly across its enterprise. 'We plan to apply AAA to every image we ingest at NGA by the end of [2018]… It is a profound change. And it is our future. And it's happening today,' asserted Cardillo.[88] Other agencies have been less enthusiastic about AAA, but this follows the pattern of early adoption seen thus far. It could be expected that further development – particularly a proof of concept – and some outside impetus may push for broader application of AAA in intelligence processing and analysis.

Intelligence agencies have always had to mine data for useful information, as the indexes and archives at Bletchley Park during World War II attest.[89] These efforts are miniscule compared to today's intelligence collection processes, and the Snowden disclosures shed light on the data volumes derived from various alleged operations.[90] According to press accounts, through its DISHFIRE project, NSA collected 200 million text messages a day in 2011.[91] An NSA spokesperson noted that 'DISHFIRE is a system that processes and stores lawfully collected SMS data', is conducted under legal oversight, and is 'focused and specifically deployed against – and only against – valid foreign intelligence targets in response to intelligence requirements.'[92]. Likewise, according to press accounts, under the FASCIA programme, the NSA logged billions of mobile phone location records per day.[93] GCHQ's OPTIC NERVE harvested webcam images from 1.8 million Yahoo! customers at rate of one every five seconds over a six-month period.[94]

In the years since these data points were established, data volumes traversing the global Internet have increased by an order of magnitude.[95] As the former Director of GCHQ, Iain Lobban, observed in 2014, however, his agency's ability to collect this data is constrained by law and by

resources.[96] Far from possessing a panoptic vision of global communications, intelligence agencies are permitted and able to see only a small sample of global traffic. This puts a premium on accelerating capability development in order, as Lobban described it, to 'access the Internet at scale', but also on analytical tools that make the most of this data bounty.

In response to the Snowden leaks, NSA set out to clarify and contextualize various collection programmes, explaining the importance of capabilities like XKEYSCORE, a system that allowed NSA analysts to cross-match and interrogate data using soft and hard 'selectors' like keywords and personal information, respectively.[97] This allowed analysts to search and reconstruct users' digital traces and relationships, including setting up alerts for future activities, facilitating the construction of individual 'fingerprints', unique records of network activity for any digital user, anywhere in the world.[98] If reports are correct, such tools are powerful means for interrogating intelligence data-sets. In a statement NSA noted that 'for example, as of 2008, there were over 300 terrorists captured using intelligence generated from XKEYSCORE.'[99]

But more is at stake in this process. As noted with NGA's vision, intelligence analysis is shifting towards new forms of knowledge production, principally through the application of big data analytics intended to extract meaning and value from massive volumes of data, either retrospectively or in real time. In addition to looking for a needle in a haystack, big data analytics also expects the haystack to yield the needle. In essence, data is increasingly being turned over to algorithms and ML to generate leads and connections, rather than being subject to human intuition and direction.[100] It has long been recognised that, '[n]o amount of raw data can substitute for an insightful human analyst able to discern the critical policy or operational significance of an event, action or trend which may be hidden within a mass of confusing and contradictory information'.[101] Machines yield correlations; humans provide insight into causality. Absent human discrimination,

big data analytics and its reliance on automated categorisation, hypothesis generation, and decision-making tend to generate many false positives, which incur additional labour costs in investigation and generate negative resource externalities.[102] There is a related issue inherent to algorithmic processes in which biases, often unintentional, are coded into algorithms and reinforced through machine-learning processes.[103] The computational sciences may yet overcome these problems and big data analytics clearly have great potential for intelligence analysis. However, it will be crucial for intelligence agencies to 'fuse the capabilities of analysts and algorithms', rather than be seduced by the promises of big data analytics.[104] For instance, NGA has sought to keep humans 'in the loop' because, according to a spokeswoman, 'It's not just going to be about technological know-how. You also need to be able to apply critical thinking because it's our responsibility to ensure that as we apply AAA sorts of capabilities to the business of GEOINT [geospatial intelligence] that we let the machines do what the machines can do, and let the humans do that which the humans are destined to do.'[105]

Another problematic area for intelligence agencies is the more introspective mission to prevent access to, or revelation of, one's own secrets. The insider threat has already been discussed, but there is also a more conventional counter-intelligence function at stake, which aims to prevent compromise of one's information assets. Historically, responsibility for information assurance (IA), once known as communications security, has rested with the SIGINT agencies. This includes the Communications-Electronics Security Group (CESG) within GCHQ and the NSA's Information Assurance Directorate.[106] As information technologies have developed, the means of penetration and defence have diversified, and intelligence agencies have been at the forefront of developing IA processes and practices. Their experience and expertise means there is an increased premium on disseminating IA knowledge outside the intelligence community; in this respect, the

remit of IA bodies is broader and further reaching than it has ever been. Institutions like the UK National Cyber Security Centre – part of GCHQ – have made important strides in modulating this type of public-private dynamic but there are other tensions between the intelligence agencies and external demands.

It is often remarked that the Internet was built for simplicity of communication, not security, and the twin problem of how to encrypt friendly communications and decrypt enemy communications on non-secure networks has long been a key research area for the intelligence community. An important step towards solving this problem was undertaken at GCHQ in the late 1960s and early 1970s but was not revealed until 1997. We now know that a small group of GCHQ cryptographers and mathematicians developed the principles of what would become known as public key encryption. The idea is straightforward: it involves the ability to compose, encrypt, send, receive and decrypt a message. The crucial element is that encryption and decryption are achieved using two different keys that have not been shared between the sender and recipient.[107] GCHQ kept this theoretical development secret, but in 1976 two American mathematicians independently discovered the same principles, published its details, and patented its practical application.[108] The tensions between intelligence encryption demands and public security stem from this period and are often characterised as 'crypto wars' in which the NSA in particular seeks to limit non-intelligence access to strong encryption. Notwithstanding these political conflicts, the subsequent development of Internet communications, banking and commerce would not have been possible without public key encryption and other cryptographic breakthroughs like RSA and Pretty Good Privacy (PGP).[109] Taken cumulatively, they have revolutionised – and further politicised – intelligence work and, initially at least, served to widen the gulf between advanced states and those with less understanding of, and access to, strong cryptography.

Intelligence collection, counter-intelligence, and analysis have always comprised a cat-and-mouse game. Cyber developments have not changed this, although most commentators agree that the cyber environment has shifted the offence-defence balance even further in favour of the attacker.[110] Conventional intelligence functions like IA and encryption have taken on increased salience under these conditions. Information technologies have also provided additional opportunities for collection that demand new modes of analysis, which, whilst ostensibly promising and beneficial, are not without their challenges. Indeed, the ability of intelligence agencies to reach into targets' lives in hitherto impossible ways has raised questions not just about legality and oversight, but about tasking and decision-making support. Which missions are necessary from a strategic security perspective? Which are being driven by technological capability or by bureaucratic competition? The answers to these questions will hold great significance regarding the legitimacy of intelligence and security agencies' roles in providing security in the twenty-first century. Although Anglo-American intelligence agencies were designed to be apolitical, the balance between legitimacy and capability (also at times constructed as 'freedom or security') will manifest itself in perceived political ways. A miscalculation of this delicate civic equation by the overseers or the agencies themselves may produce a backlash strong enough to undo much of the early adoption and integration efforts to date.

OFFENSIVE CYBER OPERATIONS

One area in particular has already occasioned discussions about the proper role of intelligence agencies in cyber affairs. This relates to an old question about whether covert or offensive actions are properly part of the intelligence process. In the United States, there has been less argument: the CIA retains a paramilitary section devoted to covert action, and who operate legally under Title

50 of the U.S. Code.[111] In the UK, the position has been less clear-cut, with operational emphasis generally lying outside the intelligence community.[112] Today, on account of their relative experience with the technical requirements of both cyber offense and defence, the United States and UK rely on their SIGINT agencies to carry out much, but not all, of their offensive cyber operations. The UK National Offensive Cyber Programme is a partnership between GCHQ and the Ministry of Defence that helps integrate cyber into joint military operations.[113] The United States relies on the NSA and its sister organisation, United States Cyber Command, which are co-located at Fort Meade. Importantly, the NSA Director is also the head of Cyber Command, providing a great deal of organisational unity across the Department of Defense. SIGINT agencies in both countries are therefore deeply involved in developing offensive cyber capabilities and in running offensive cyber operations, whether for purposes of espionage (computer network exploitation, CNE), or sabotage and degradation (computer network attack, CNA).

Much has been claimed of the game-changing role of 'cyber weapons' in peace and war. According to journalist and author Kim Zetter, the Stuxnet worm that compromised Iranian nuclear enrichment operations was part of a combined U.S.-Israeli covert operation to bring Iran to the negotiating table.[114] It achieved this but only as part of a broader suite of statecraft instruments. The independent efficacy of cyber weapons in generating strategic effect, particularly as a tool of covert coercion, is somewhat unproven,[115] and secrecy and counterfactual analysis of monocausal claims make conclusions difficult. In the operational military context, former Secretary of Defense Ash Carter confessed to being 'disappointed' in the use of cyber weapons against ISIS.[116] This was partly because intelligence agencies did not wish to deploy cyber weapons in case their intelligence collection was negatively affected. However, Carter's analysis of the efficacy of cyber weapons in the counter-ISIS campaign must be updated to account for the recently declassified

documents that indicate successes by Cyber Command's Joint Task Force Ares in denying ISIS operational use of the cyber domain.[117]

There is, however, no doubt that cyber is being integrated into military and espionage operations across the board, and intelligence agencies are playing a central role in this evolution. Covert cyber operations are a component of the arsenal of dozens of states and their perceived utility will continue to drive their development and deployment. The UK has been bullish about its sovereign capabilities and in 2013 became the first country in the world to admit to developing an offensive cyber capability.[118] The United States has developed similar cyber capabilities, but the Obama administration was hesitant to grant authorities to unleash the capabilities. The Trump administration, for its part, has indicated strongly its willingness to bring offensive cyber to the fore in its foreign policy and military and intelligence operations.[119] In September 2018, National Security Advisor John Bolton captured this difference in approach, stating, 'We're going to do a lot of things offensively, and our adversaries need to know that…we're not just on defense as we have been.' Likewise, Cyber Command's Deputy Commander testified to Congress: 'If you had approached me six months ago about the limits of our authorities I would tell you that it caused me great frustration…We're in a much better place today.'[120]

The attraction of offensive cyber operations is similar to that which has motivated military and intelligence agencies for decades: the ability to launch a precision strike at distance, thereby maximising force protection and minimising political fallout.[121] Cyber operations are also sometimes perceived as relatively cheap and easy. This may be true at the lower end of the capability spectrum, but high-grade capabilities require significant investment of time and effort that belies their facile characterisation as only one keystroke away from deployment and seemingly

instant success. Indeed, persistent access while remaining hidden on a network can be as challenging as gaining access in the first place.

The research and development costs of developing cyber weapons can be considerable, albeit not nearly as great as with conventional and nuclear arms.[122] Whilst this demonstrates resolve and capability to adversaries, they are difficult to use well. Intelligence agencies know this and protect their capabilities, not least as once deployed they allow adversaries to patch their vulnerabilities and to reverse-engineer cyber tools used against them.[123] Despite the lack of explicit international law regulating offensive cyber capabilities, states are generally quite restrained in their use, fearing exposure and escalation if they do, as well as normalising their deployment by adversaries.[124] Still, how these norms will develop in an anarchic international system has been the study of much discussion, but little agreement.[125]

There are of course many notable differences between cyber weapons and other weapons classes, but the reasons for their development and deployment are roughly the same: to generate strategic effect against another state or non-state actor. Covert intelligence operations in the form of CNE and especially CNA are key to this endeavour and, whilst their efficacy is perhaps over stated, they have clear potential in pursuing national and alliance interests. However, challenges remain in developing ethical, legal and normative frameworks for intelligence use of these capabilities. Importantly, the lines between CNE and CNA are often indistinct, blurring already fuzzy categories of offence and defence, with ramifications for escalation management and strategic stability.[126] This exacerbates the long-standing tension between the stabilizing effects of intelligence on international relations and the potentially destabilizing modes of its collection.[127]

CHANGING ROLES AND REQUIREMENTS OF INTELLIGENCE

There is little doubt that the shifting technological conditions of the modern world have always brought about changes in intelligence priorities and practices. Developments in computing and communications have provided both opportunities and constraints for intelligence agencies, although few would argue that the latter outweigh the former. Intelligence has, in an important sense, never been in ruder health. There are distinct challenges inherent in an expanding attack surface that exposes vulnerabilities to exploitation and subversion, but the sheer volume and variety of intelligence sources has been a boon to intelligence agencies worldwide despite the increasingly complex political considerations in the U.S. and the UK. We are even debating whether we need to develop new forms of intelligence to accommodate these developments, such as social media intelligence (SOCMINT) and cyber intelligence (CYBINT).[128] Intelligence agencies have reorganised before to better cope with the demands of the information age.[129] They are doing so again to deal with cyber, through new institutions, new capabilities, and new ways of thinking, as with big data analytics, and with norms governing 'digital intelligence'.[130] These occur against the backdrop of wider governmental restructuring to bring a properly strategic approach to cybersecurity in general.

This latter aspect is related to broader changes in the intelligence environment. In the UK, for instance, there has been a shift from the primary protection of the state to a more expansive concern with protecting society and the individuals that comprise it.[131] The intelligence remit has therefore grown to focus on individuals as much as on friendly and enemy states. In this context, some forms of digital intelligence collection, for example, so-called 'bulk powers', have often been characterised as mass surveillance, a charge rejected by intelligence agencies and others.[132] The links and public awareness among classic intelligence functions, societal security and

resilience have also intensified, meaning that the role of cyber within government has changed, bringing together and cutting across multiple sectors as it does.

Indeed, there remains the conventional panoply of post-Cold War national security challenges, from terrorism and organised crime to narcotics trafficking, from information warfare to weapons proliferation, and the cyber dimension has impacted and complicated these seemingly disparate threats in alarming ways.[133] The major implication of this is that government departments have to work together, often in novel ways, to address cross-cutting areas of concern. It is now a demonstrable marker of a responsible state to publish a national cyber security strategy, which coordinates government agencies and departments and interactions with private firms and civil society.[134] Several dozen states and regional and international organisations have done just this. In almost all cases, intelligence occupies a central role and is required to be a source of competence and capability, a driver of change, and responsive to shifting political agendas.

The hyper-connectivity of global information networks and contemporary societies is one of the greatest technological developments in human history and merits the revolutionary moniker that is endemic amongst many observers. It has resulted in profound changes to society, conceptions of national security, and, by extension, to intelligence work. Despite this, the central rationale for intelligence bureaucracies has barely altered even as their collection types have indeed expanded since the term cyber entered the vernacular. Gathering information on an adversary that they wish to remain secret, using that knowledge to narrow the cone of uncertainty for decision-makers, and doing so without being detected remain the cornerstones of intelligence. From a narrower covert action perspective, however, cyber has given actors a powerful new tool that remains tempting to use in the absence of appealing alternatives, but remains fraught in its employment.

Given this analysis of historical patterns of technology and intelligence, we must conclude that the cyber era is a technological revolution, but not an intelligence revolution. To use the cyber revolution to support policymakers and military commanders with enhanced operational and analytical capability in and through cyberspace, intelligence communities must follow their own precedents in integrating cyber into traditional collection and analysis efforts. As we have illustrated, some have done this to great effect already, but these developments have been interrupted by counterintelligence failures and muddled political oversight, some of which have been the result of insider threats acting in response to concerns over the secret application of powerful technology.

No matter how such questions come to the fore, concerns over societal disruption and questions of legitimacy have caused political overseers to put policy and legal brakes on raw intelligence capabilities, potentially artificially retarding what might otherwise be fairly characterised as a revolution if the speed of change was left unchecked. While such considerations are being grappled with in the Anglo-American context, authoritarian states have shown no such restraint in capability development to consider the ways in which they are adapting their own intelligence apparatuses to benefit from the cyber revolution. If normative considerations occupy only liberal states, the cyber capability gap could narrow with significant implications for international security. Perhaps the revolution in intelligence is yet to come.

---

[1] James Stavridis, "The United States is not ready for a Cyber-Pearl Harbor," 15 May 2017, accessed at https://foreignpolicy.com/2017/05/15/the-united-states-is-not-ready-for-cyber-pearl-harbor-ransomware-hackers-wannacry/, 13 December 2018.
[2] Suzanne Kelly, "Are We Headed for a 'Cyber Cuban Missile Crisis' with Russia?" 5 June 2018, accessed at https://www.thecipherbrief.com/are-we-headed-for-a-cyber-cuban-missile-crisis-with-russia, 13 December 2018.
[3] For a review, see Hans-Inge Langø, "Competing Academic Approaches to Cyber Security," in Karsten Friis and Jens Ringsmose, eds., *Conflict in Cyberspace: Theoretical, Strategic and Legal Perspectives* (Abingdon: Routledge, 2016), 7-26.

[4] On the problematic gap between technical and non-technical contributions, see PW Singer and Allan Friedman, *Cybersecurity and Cyberwar: What Everyone Needs to Know* (New York: Oxford University Press, 2014), 4-8.
[5] Brandon Valeriano, Benjamin Jensen and Ryan C. Maness, *Cyber Strategy: The Evolving Character of Power and Coercion* (New York: Oxford University Press, 2018).
[6] David Barnard-Wills and Debi Ashenden, "Securing Virtual Space: Cyber War, Cyber Terror and Risk," *Space and Culture* 15 (May 2012): 110-23.
[7] Michael Sulmeyer, "Much Ado About Nothing? Cyber Command and the NSA," *War on the Rocks*, 19 July 2017, accessed at https://warontherocks.com/2017/07/much-ado-about-nothing-cyber-command-and-the-nsa/, 10 March 2018.
[8] They have not been ignored, however. See, Frederick Wettering, "The Internet and the Spy Business," *International Journal of Intelligence and Counterintelligence* 14 (October 2001): 342-65; William Nolte, "Keeping Pace with the Revolution in Military Affairs: Operation Iraqi Freedom and the Challenge to Intelligence," *CIA Studies in Intelligence* 48 (Winter-Spring 2004): 1-10; John Ferris, "Netcentric Warfare, C4ISR and Information Operations: Towards a Revolution in Military Intelligence?" *Intelligence and National Security* 19 (Summer 2004): 199-225; Arthur Hulnick, "Intelligence Producer-Consumer Relations in the Electronic Era," *International Journal of Intelligence and Counterintelligence* 24 (September 2011): 747-56; Michael Warner, "Reflections on Technology and Intelligence Systems," *Intelligence and National Security* 27 (February 2012): 133-53; Michael Warner, "Cybersecurity: A Pre-History," *Intelligence and National Security* 27 (October 2012): 781-99; Aaron Brantly, "Defining the Role of Intelligence in Cyber: A Hybrid Push and Pull," in Mark Phythian, ed., *Understanding the Intelligence Cycle* (Abingdon: Routledge, 2013), 76-98; Nigel Inkster, "Chinese Intelligence in the Cyber Age," *Survival* 55(February-March 2013): 45-66; Joshua Rovner, "Intelligence in the Twitter Age," *International Journal of Intelligence and Counterintelligence* 26 (February 2013): 260-71; Martin Rudner, "Cyber-Threats to Critical National Infrastructure: An Intelligence Challenge," *International Journal of Intelligence and Counterintelligence* 26 (May 2013): 453-81; Troy Mattern, John Felker, Randy Borum and George Bamford, "Operational Levels of Cyber Intelligence," *International Journal of Intelligence and Counterintelligence* 27 (October 2014): 702-19; Ross Bellaby, "Justifying Cyber-Intelligence?" *Journal of Military Ethics* 15 (October-December 2016): 299-319; Stephen Gary and Randy Borum, "Evolving Cyber Intelligence," in Damien van Puyvelde and Aaron Brantly, eds., *U.S. National Cybersecurity: International Politics, Concepts and Organization* (Abingdon: Routledge, 2017), 123-39; Aaron Brantly, *The Decision to Attack: Military and Intelligence Cyber Decision-Making* (Athens, GA: University of Georgia Press, 2018); David Omand, "The Threats from Modern Digital Subversion and Sedition," *Journal of Cyber Policy* 3 (May 2018): 5-23.
[9] John Ferris, 'Netcentric Warfare, C4ISR and Information Operations: Towards a Revolution in Military Intelligence?', *Intelligence and National Security* 19 (2004): 199-225.
[10] On the impact of technology in military revolutions throughout history, see Max Boot, *War Made New: Technology, Warfare, and the Course of History, 1500 to Today* (New York: Gotham Books, 2007).
[11] See, Eric Denece, 'The Revolution in Intelligence Affairs: 1989-2003', *International Journal of Intelligence and Counterintelligence* 27 (2014): 27-41.
[12] Deborah G. Barger, 'Toward a Revolution in Intelligence Affairs', *RAND Corporation Technical Report*, 2005, p. vii, accessed at https://apps.dtic.mil/dtic/tr/fulltext/u2/a448571.pdf
[13] Ferris, p. 199ff.
[14] William J. Lahneman, 'Is a Revolution in Intelligence Affairs Occurring?, *International Journal of Intelligence and Counterintelligence* 20 (2007): 1-17.
[15] Lucas Kello, *The Virtual Weapon and International Order* (New Haven: Yale University Press, 2017), p.257. See also 'The Meaning of the Cyber Revolution', *International Security* 38 (Fall 2013): 7-40.
[16] Warner, "Reflections on Technology,"135, original emphasis.
[17] David Omand, "Into the Future: A Comment on Agrell and Warner," *Intelligence and National Security* 27 (February 2012): 154-6.
[18] See, Daniel Headrick, *The Invisible Weapon: Telecommunications and International Politics, 1851-1945* (New York: Oxford University Press, 1991), 117.
[19] Headrick, *Invisible Weapon*, 117-119.
[20] John Johnson, *The Evolution of British SIGINT, 1653-1939* (Cheltenham: HMSO, 1997). Signals intelligence (SIGINT) is 'the interception of the communications of others (states, armies, companies, etc.)'; Peter Gill and Mark Phythian, *Intelligence in an Insecure World*, third edn. (Cambridge: Polity Press, 2018), 53.
[21] John Ferris, "Before Room 40: The British Empire and Signals Intelligence, 1898-1914," *Journal of Strategic Studies* 12 (September-December 1989): 431-57.
[22] W.J. Baker, *A History of the Marconi Company* (London: Methuen, 1970).

[23] Peter Freeman, "MI1(b) and Origins of British Diplomatic Cryptanalysis," *Intelligence and National Security* 22 (April 2007): 206-28, at 209.
[24] Freeman, "MI1B."
[25] John Ferris, "The Road to Bletchley Park: The British Experience with Signals Intelligence, 1892-1945," *Intelligence and National Security* 17 (April 2002): 53-84.
[26] Warren Kimball, ed., *Churchill and Roosevelt: The Complete Correspondence: Volume 1, Alliance Emerging October 1933-November 1942* (Princeton, NJ: Princeton University Press, 1984), 9.
[27] Quoted in Ferris, "The Road to Bletchley Park," 72.
[28] Ferris, "The Road to Bletchley Park," 75.
[29] FH Hinsley and Alan Stripp, eds., *Codebreakers: The Inside Story of Bletchley Park* (Oxford: Oxford University Press, 1993).
[30] Walter McDougall, *The Heavens and the Earth: A Political History of the Space Age* (Baltimore, MD: Johns Hopkins University Press, 1985).
[31] For a discussion of intelligence technologies during the Cold War, see Michael Warner, *The Rise and Fall of Intelligence: An International Security History* (Washington, DC: Georgetown University Press, 2014), chap. 4.
[32] David Gioe, "Handling HERO: Joint Anglo-American Tradecraft in the Case of Oleg Penkovsky," in David Gioe, Len Scott, and Christopher Andrew, eds., *An International History of the Cuban Missile Crisis* (Abingdon, UK: Routledge), 135-175.
[33] Gioe, "Handling HERO."
[34] Kim Zetter, *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon* (New York: Broadway Books, 2015).
[35] Michael S Goodman, *Spying on the Nuclear Bear: Anglo-American Intelligence and the Soviet Bomb* (Stanford, CA: Stanford University Press, 2007), 12ff.
[36] Jeffrey Richelson, *The Wizards of Langley: Inside the CIA's Directorate of Science and Technology* (London: Basic Books, 2008).
[37] Michael S. Goodman, "Jones' Paradigm: The How, Why, and Wherefore of Scientific Intelligence," *Intelligence and National Security* 24 (April 2009): 236-56.
[38] Sean Lyngaas, "Inside the CIA's new Digital Directorate," 1 October 2015, accessed at https://fcw.com/articles/2015/10/01/cia-digital-directorate.aspx, 13 December 2018.
[39] Paul Edwards, *The Closed World: Computers and the Politics of Discourse in Cold War America* (Cambridge, MA: MIT Press, 1996), 15.
[40] Nick Cullather, "Bombing at the Speed of Thought: Intelligence in the Coming Age of Cyberwar," *Intelligence and National Security* 18 (Winter 2003): 141-54.
[41] James William Gibson, *The Perfect War: The War We Couldn't Lose and How We Did* (New York: Vintage, 1986). See also, Antoine Bousquet, *The Scientific Way of Warfare: Order and Chaos on the Battlefields of Modernity* (London: Hurst & Company, 2009).
[42] Warner, *The Rise and Fall of Intelligence*, 164-5.
[43] Office of the Historian of the U.S. Department of State, "U-2 Overflights and the Capture of Francis Gary Powers, 1960," publication date unknown, accessed at https://history.state.gov/milestones/1953-1960/u2-incident, 14 December 2018.
[44] Mark Lundstrom, "Moore's Law Forever?" *Science* 299 (January 2003): 210-11.
[45] Omand, "Into the Future," 155.
[46] Lawrence Krauss, *Quantum Man: Richard Feynman's Life in Science* (London: W.W. Norton, 2012).
[47] Janet Abbate, *Inventing the Internet* (Cambridge, MA: MIT Press, 1999).
[48] On the idea that technology affects the tasking and organisation of intelligence, see Michael Warner, "Building a Theory of Intelligence Systems," in Gregory Treverton and Wilhelm Agrell (eds.), *National Intelligence Systems: Current Research and Future Prospects* (Cambridge: Cambridge University Press, 2009), 11-37.
[49] Desmond Bristow, *A Game of Moles: The Deceptions of an MI6 Officer* (London: Little, Brown, 1993).
[50] Christopher Andrew and Vasili Mitrokhin, *The KGB in Europe and the West: The Mitrokhin Archive* (London: Penguin, 2000).
[51] Wayne Barker and Rodney Coffman, *The Anatomy of Two Traitors: The Defection of Bernon F. Mitchell and William H. Martin* (Laguna Hills, CA: Aegean Press, 1981).
[52] Winslow Peck, "U.S. Electronic Espionage: A Memoir," *Ramparts* 11 (August 1972): 35-50, accessed at http://cryptome.org/jya/nsa-elint.htm, 14 April 2018.
[53] For example, Oleg Gordievsky revealed that almost half his KGB agents specialised in communications. See, Wettering, "Internet and the Spy Business," 342.

[54] Clifford Stoll, *The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage* (New York: Doubleday, 1989).
[55] *Learning from the Enemy: The GUNMAN Project*, https://www.nsa.gov/about/cryptologic-heritage/historical-figures-publications/publications/assets/files/gunman-project/Learning_From_the_Enemy_The_GUNMAN_Project.pdf. See Warner, "Cybersecurity," 786-7, on United States government concerns about computer security from the early 1980s.
[56] Wayne Madsen, "Intelligence Agency Threats to Computer Security," *International Journal of Intelligence and Counterintelligence*, 6 (Winter 1993): 413-88, at 419.
[57] Abbate, *Inventing the Internet*.
[58] Tim Berners-Lee and Mark Fischetti, *Weaving the Web: The Original Design and Ultimate Destiny of the World Wide Web by Its Inventor* (New York: Harper Collins, 1999).
[59] Frank Webster, *Theories of the Information Society* (Abingdon: Routledge, 2014).
[60] For an historical contextualisation of these dynamics, see David Betz, *Carnage and Connectivity: Landmarks in the Decline of Conventional Military Power* (London: Hurst & Company, 2015).
[61] Michael Hayden, speech to Aspen Security Forum, 29 July 2011, accessed at https://www.youtube.com/watch?v=yoWkAVXmSs0, 12 May 2018.
[62] Tim Stevens, *Cyber Security and the Politics of Time* (Cambridge: Cambridge University Press, 2016), 68-73.
[63] Richard Aldrich, "Beyond the Vigilant State: Globalisation and Intelligence," *Review of International Studies* 35:4 (October 2009): 889-902.
[64] See, United States Senate, Committee on Armed Services, "Cyber-Enabled Information Operations," 27 April 2017, accessed at https://www.armed-services.senate.gov/imo/media/doc/17-37_04-27-17.pdf, 20 March 2019.
[65] David Murakami Wood and Steve Wright, "Before and After Snowden," *Surveillance and Society* 13 (July 2015): 132-8.
[66] Loch Johnson, Richard Aldrich, Christopher Moran, David Barrett, Glenn Hastedt, Robert Jervis, Wolfgang Krieger, Rose McDermott, David Omand, Mark Phythian and Wesley Wark, "An *INS* Special Forum: Implications of the Snowden Leaks," *Intelligence and National Security* 29 (November-December 2014): 793-810.
[67] For example, the USA Freedom Act, HR 2048, 2015 and Investigatory Powers Act 2016.
[68] See M Lowenthal, *Intelligence: From Secrets to Policy* (Washington, DC: CQ Press, 2014).
[69] James Gosler, "The Digital Dimension," in Jennifer Sims and Burton Gerber, eds., *Transforming U.S. Intelligence* (Washington, DC: Georgetown University Press, 2005), 96.
[70] David V. Gioe, "'The More Things Change': HUMINT in the Cyber Age," in Robert Dover, Huw Dylan, and Michael S. Goodman, eds., *The Palgrave Handbook of Security, Risk, and Intelligence* (London: Palgrave Macmillan, 2017), 213-228.
[71] Brendan Koerner, "Inside the Cyberattack that Shocked the U.S. Government," *Wired*, 23 October 2016, accessed at https://www.wired.com/2016/10/inside-cyberattack-shocked-us-government/, 20 March 2019
[72] Ellen Nakashima, 'Hacks of OPM Databases Compromised 22.1 Million People, Federal Authorities Say', *The Washington Post* (9 July 2015).
[73] Hannah Kuchler, "Chinese Hackers May be Mapping U.S. Government," *Financial Times*, 7 June 2015, accessed at https://www.ft.com/content/3c2dd3e8-0bdd-11e5-a06e-00144feabdc0, 20 March 2019
[74] Valeriano et al., *Cyber Strategy*, 154.
[75] FH Hinsley, "The Influence of ULTRA in the Second World War," in FH Hinsley and Alan Stripp, eds., *Codebreakers: The Inside Story of Bletchley Park* (Oxford: Oxford University Press, 1993), 233, 144.
[76] Ralph Bennett, *Behind the Battle: Intelligence in the War with Germany, 1939-45* (London: Sinclair-Stevenson, 1994), 278.
[77] David Stafford, *Spies Beneath Berlin* (London: Thistle Publishing, 2013).
[78] Wettering, "Internet and the Spy Business," 349.
[79] See, Andy Greenberg, "Snowden: I Left the NSA Clues, But They Couldn't Find Them," *Wired*, 13 August 2014, accessed at https://www.wired.com/2014/08/snowden-breadcrumbs/, 20 March 2019.
[80] David Anderson, *A Question of Trust: Report of the Investigatory Powers Review*, June 2015, 44, accessed at https://terrorismlegislationreviewer.independent.gov.uk/wp-content/uploads/2015/06/IPR-Report-Web-Accessible1.pdf, 20 March 2019.
[81] Chase Madar, *The Passion of Bradley Manning: The Story Behind the Wikileaks Whistleblower* (London: Verso, 2013).
[82] "Director Pompeo Delivers Remarks at CSIS," 13 April 2017, accessed at https://www.cia.gov/news-information/speeches-testimony/2017-speeches-testimony/pompeo-delivers-remarks-at-csis.html., 24 June 2018.
[83] David Lyon, *Surveillance Society: Monitoring Everyday Life* (Buckingham: Open University Press, 2001), 39.

[84] Tom Harper, Richard Kerbaj and Tim Shipman, "British Spies Betrayed to Russians and Chinese," *The Sunday Times*, 14 June 2015.
[85] David V. Gioe, "Tinker, Tailor, Leaker, Spy: The Future Costs of Mass Leaks," *The National Interest* 129 (January/February 2014): 51-59.
[86] Tim Stevens, "Peak Performance: Inter-State HPC Competition Intensifies," *Jane's Intelligence Review* 29 (November 2017): 46-9.
[87] *Jane's Intelligence Review*, "Machine Learning Advances Intelligence Analysis,"2018, accessed at https://www.janes.com/images/assets/568/79568/Machine_learning_advances_intelligence_analysis.pdf, 14 December 2018.
[88] Samantha Ehlinger, "NGA prepares for a future of AI-supported intelligence,"*FedScoop*, 26 April 2018, accessed at https://www.fedscoop.com/nga-prepares-future-ai-supported-intelligence/, 15 December 2018.
[89] Rodney Brunt, "Indexes at the Government Code and Cypher School, Bletchley Park, 1940-1945," in W. Boyd Rayward and Mary Ellen Bowden (eds.), *The History and Heritage of Scientific and Technological Information Systems* (Medford, NJ: Information Today, 2004), 291-9.
[90] Anderson, *A Question of Trust*, 330-1.
[91] James Ball, "NSA Collects Millions of Text Messages Daily in 'Untargeted' Global Sweep", *The Guardian*, 16 January 2014, accessed at https://www.theguardian.com/world/2014/jan/16/nsa-collects-millions-text-messages-daily-untargeted-global-sweep.
[92] Ball, "NSA Collects Millions of Text Messages Daily."
[93] Paul Szoldra, "Leaked NSA Document Says Metadata Collection is One of Agency's 'Most Useful Tools'," *Business Insider*, 7 December 2016, accessed at https://www.businessinsider.com/nsa-document-metadata-2016-12, 20 March 2019.
[94] Spencer Ackerman and James Ball, "Optic Nerve: Millions of Yahoo Webcam Images Intercepted by GCHQ," *The Guardian*, 28 February 2014, accessed at https://www.theguardian.com/world/2014/feb/27/gchq-nsa-webcam-images-internet-yahoo, 20 March 2019.
[95] See Cisco's Visual Networking Index Global Fixed and Mobile Internet Traffic Forecasts, accessed at https://www.cisco.com/c/en/us/solutions/service-provider/visual-networking-index-vni/index.html, 20 March 2019.
[96] Gordon Corera, "GCHQ's Outgoing Director Warns Spies Must Monitor the Internet," *BBC News*, 21 October 2014, accessed at https://www.bbc.co.uk/news/uk-29708493, 12 April 2018.
[97] "NSA Press Statement in Response to Allegations about NSA Operations," 30 July 2013, accessed at https://www.nsa.gov/news-features/press-room/Article/1618731/nsa-press-statement-in-response-to-allegations-about-nsa-operations/, 20 March 2019.
[98] Glenn Greenwald, "XKeyscore: NSA Tool Collects 'Nearly Everything a User Does on the Internet'," *The Guardian*, 31 July 2013, accessed at https://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data, 20 March 2019.
[99] NSA Press Statement.
[100] Kevjn Lim, "Big Data and Strategic Intelligence," *Intelligence and National Security* 31 (Autumn 2016): 619-35.
[101] Alan Dupont, "Intelligence for the Twenty-First Century," *Intelligence and National Security* 18 (Winter 2003): 15-39, at 22.
[102] Claudia Aradau and Tobias Blanke, "The (Big) Data-Security Assemblage: Knowledge and Critique," *Big Data and Society* 2 (October 2015), doi: 10.1177/2053951715609066.
[103] Keith Kirkpatrick, "Battling Algorithmic Bias," *Communications of the ACM* 59 (September 2016): 16-17.
[104] Christopher Eldridge, Christopher Hobbs and Matthew Moran, "Fusing Algorithms and Analysts: Open-Source Intelligence in the Age of 'Big Data'," *Intelligence and National Security* 33 (Spring 2018): 391-406, at 401.
[105] Ehlinger, "NGA Prepares for a Future of AI-Supported Intelligence."
[106] In 2016, CESG was absorbed by the National Cyber Security Centre, also part of GCHQ.
[107] For a detailed history and explanation of public key encryption and its effects, see Thomas Rid, *Rise of the Machines: A Cybernetic History* (New York: W.W. Norton, 2016), 246-93
[108] Whitfield Diffie and Martin Hellman, "New Directions in Cryptography," *IEEE Transactions on Information Theory* 22 (November 1976): 644-54.
[109] RSA is another form of public key encryption developed in the 1970s to encrypt and decrypt digital messages; PGP (Pretty Good Privacy) was released in 1991 and built upon RSA and other protocols to provide even more secure communications. On the development and significance of these encryption programs and the response of the security and intelligence community, see Steven Levy, *Crypto: How the Code Rebels Beat the Government–Saving Privacy in the Digital Age* (New York: Penguin Books, 2001).

[110] Rebecca Slayton, "What is the Cyber Offense-Defense Balance? Conceptions, Causes, and Assessment," *International Security* 41 (Winter 2016/17): 72-109.
[111] Loch Johnson, "Covert Action and Accountability: Decision-Making for America's Secret Foreign Policy," *International Studies Quarterly* 33 (March 1989): 81-109.
[112] Rory Cormac, "Coordinating Covert Action: The Case of the Yemen Civil War and the South Arabian Insurgency," *Journal of Strategic Studies* 36 (October 2013): 692-717.
[113] HM Government, *National Cyber Security Strategy 2016-2021*, November 2016, accessed at *https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf*, 20 March 2019, 51; see also, Intelligence and Security Committee of Parliament, *Annual Report 2016-2017*, December 2017, accessed at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/727949/ISC-Annual-Report-2016-17.pdf, 20 March 2019, 43-5.
[114] Kim Zetter. *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon* (New York: Broadway Books, 2014).
[115] Valeriano et al., *Cyber Strategy*.
[116] Ashton Carter, *A Lasting Defeat: The Campaign to Destroy ISIS* (Cambridge, MA: Belfer Center for Science and International Affairs, 2017), 33.
[117] Michael Martelle, "Joint Task Force ARES and Operation GLOWING SYMPHONY: Cyber Command's Internet War Against ISIL" *National Security Archive*, 13 August 2019, accessed at https://nsarchive.gwu.edu/briefing-book/cyber-vault/2018-08-13/joint-task-force-ares-operation-glowing-symphony-cyber-commands-internet-war-against-isil
[118] James Blitz, "UK Becomes First State to Admit to Offensive Cyber Attack Capability," *Financial Times*, 29 September 2013, accessed at https://www.ft.com/content/9ac6ede6-28fd-11e3-ab62-00144feab7de, 25 May 2018.
[119] Chris Bing, "National Security Council Delays Publication of Cyber Strategy Over Inclusion of "Offensive Measures," *CyberScoop*, 15 May 2018, accessed at https://www.cyberscoop.com/white-house-cyber-strategy-national-security-council-offensive-measures/, 20 March 2019.
[120] Martin Matishak, "A Decade after Russia Hacked the Pentagon, Trump Unshackles Cyber Command," 29 November 2018, accessed at https://www.politico.com/story/2018/11/29/a-decade-after-russia-hacked-the-pentagon-trump-unshackles-cyber-command-961103, 15 December 2018.
[121] Thomas G. Mahnken, "Weapons: The Growth and Spread of the Precision-Strike Regime," *Daedalus* 140 (Summer 2011): 45-57.
[122] Data on cyber weapons research and development costs are not available but analysts unanimously conclude that, whilst not cheap, they cost less than traditional military capabilities. A typical statement reads, 'It is unclear how much the Stuxnet program cost, but it was almost certainly less than the cost of a single fighter-bomber'; James P. Farwell and Rafal Rohozinski, "Stuxnet and the Future of Cyber War," *Survival* 53 (February-March 2011): 23-40, at 35.
[123] Thomas Rid and Peter McBurney, "Cyber-Weapons," *The RUSI Journal* 157 (February-March 2012: 6-13.
[124] Tim Stevens, "Global Code: Power and the Weak Regulation of Cyberweapons," in Nik Hynek, Ondrej Ditrych and Vit Střítecký, eds., *Regulating Global Security: Insights from Conventional and Unconventional Regimes* (Basingstoke: Palgrave Macmillan, 2019), 271-95.
[125] Alex Grigsby, "The United Nations Doubles Its Workload on Cyber Norms, and Not Everyone is Pleased," 15 November 2018, accessed at https://www.cfr.org/blog/united-nations-doubles-its-workload-cyber-norms-and-not-everyone-pleased, 15 December 2018. See also the Cyber Norms Index offered by the Carnegie Endowment for International Peace, accessed at https://carnegieendowment.org/publications/interactive/cybernorms, 20 March 2019.
[126] Ben Buchanan, *The Cybersecurity Dilemma: Hacking, Trust, and Fear Between Nations* (London: Hurst & Company, 2016).
[127] Michael Herman, *Intelligence Power in Peace and War* (Cambridge: Cambridge University Press, 1996).
[128] See David Omand, Jamie Bartlett and Carl Miller, "Introducing Social Media Intelligence (SOCMINT)," *Intelligence & National Security* 27 (December 2012): 801-23; Matteo Bonfanti, "Cyber Intelligence: In Pursuit of a Better Understanding for an Emerging Practice," *Cyber, Intelligence and Security* 2 (May 2018): 105-21.
[129] For example, David Pepper, "The Business of SIGINT: The Role of Modern Management in the Transformation of GCHQ," *Public Policy and Administration* 25 (January 2010): 85-97.
[130] David Omand, *Understanding Digital Intelligence and the Norms that Should Govern It* (London: Chatham House/CIGI, 2015), accessed at https://www.cigionline.org/publications/understanding-digital-intelligence-and-norms-might-govern-it, 20 March 2019.

[131] Peter Hennessy ed., *The New Protective State: Government, Intelligence and Terrorism* (London: Continuum, 2008); David Omand, *Securing the State* (New York: Columbia University Press, 2010).
[132] For example, '[I]t should be plain that the collection and retention of data in bulk does not equate to so-called "mass surveillance"'; David Anderson, *Report of the Bulk Powers Review*, August 2016, accessed at https://terrorismlegislationreviewer.independent.gov.uk/wp-content/uploads/2016/08/Bulk-Powers-Review-final-report.pdf, 20 March 2019, 4..
[133] On complicating existing threats, see Joel Brenner, *America the Vulnerable: Inside the New Threat Matrix of Digital Espionage, Crime, and Warfare* (New York: The Penguin Press, 2011).
[134] 'CMM Dimension 1: Cybersecurity Policy and Strategy', accessed at https://www.sbs.ox.ac.uk/cybersecurity-capacity/content/cmm-dimension-1-cybersecurity-policy-and-strategy-0, 20 March 2019.