CHAPTER 9

The Ethical Challenge of Information Warfare: Nothing New

By Graham Fairclough

This chapter considers the ethical challenge of a problem that was not new in 1914, had not been resolved by 1918, and continues to exist: the strategic weaponization of information as an instrument of war. It describes how Great Britain used its global cable and high-powered network in conjunction with its cryptographic expertise and military assets to conduct a highly successful information war campaign against Germany and its allies. The interception of the now famous Zimmermann Telegram, which many historians and analysts see as critical to the U.S. entry into the conflict in 1917, is *the* focal event.[1] Drawing on the experiences of Britain's 1914–1918 information war, this chapter next draws out five challenges that states continue to face in the increasingly ubiquitous domain of cyberspace.

Technology and the Changing Character of War

One of the most momentous aspects of World War I, as is frequently the case in all wars, was the weaponization of new and emerging technology and its use on the battlefield—the tank and airplane being those that come most readily to mind. Technological developments changed the character of war and led to these developments being described as the first *modern* conflict.[2] Another technology that impacted the character of the war significantly

was what is now referred to as information and communications technology (ICT), represented in 1914 by the cable telegraph, cable telephone, and high-powered wireless network.[3] This technology enabled the passage of information across significant distances and at a speed that far outstripped that of the carrier pigeon, dispatch rider, or ship. States that possessed these capabilities could conduct war on a global footing and could, for the first time, weaponize information through their ability to use the technology to achieve strategic effect against an adversary. Strategic information warfare had not only become possible, but its conduct influenced the outcome and the character of the Great War as well. Similarly, today's ICT, manifested in the recently defined fifth operating domain of cyberspace, is frequently cited as changing the outcome of conflict.[4]

Information War

It is important to be clear on how information warfare is defined in this chapter. In 1914, no formal definition of what today is recognized as information warfare existed,[5] although Great Britain did recognize the importance of the passage of information and the need to defend the cable and wireless networks that it passed through during war.[6] Furthermore, it is highly unlikely that any conceptualization of it as a means to achieve strategic intent had been considered by the politicians and generals planning the war. At the time, the actions taken by Britain and other states, including Germany, related to the strategic weaponization of information were perceived to be nothing more than a means to an end, comparable to the use of an artillery barrage or a naval blockade to restrict enemy maneuver.

Today, a wide spectrum of definitions of the concept exists. These range from John Arquilla's 1995 offering, "striking at communications nodes and infrastructures," to that more recently stated by Mariarosaria Taddeo, "a spectrum of phenomena, encompassing cyber-attacks as well as the deployment of robotic-weapons and ICT-based communication protocols [malware]."[7] The most fitting definition for this chapter is that presented by Winn Schwartau, "a conflict in which information and

information systems act as both weapons and the targets."[8] This definition reflects the approach taken by Britain a century ago, consisting of physical attacks made against Germany's cable and wireless networks and the use of the information transmitted through these networks to deliver effects in pursuit of its strategic objectives.[9] These effects were control, intelligence, and influence.[10]

Tactical Information Warfare in World War I

At this point, brief mention must be made of the information war that took place throughout the war at the tactical level. Activity was undertaken by each of the protagonists to obtain intelligence on adversary future intent, order of battle, and disruption of communications networks. These requirements were met through wireless intercept and direct access to telephone and telegraph cables.[11] On the Eastern Front, it was instrumental in the Russian defeat at Tannenberg in 1914—the first battle "in the history of man in which the interception of enemy radio traffic played a decisive role."[12] In the Middle East, Sir Frederick Stanley Maude credited it with providing 30 percent of his intelligence requirements during his campaign in Iraq, while Polly Mohs viewed it as having played an important role in putting down the 1915–1918 Arab revolt through its integration with small mobile indigenous forces, leading her to describe the campaign as the first modern intelligence war.[13] On the Western Front, it proved critical in preventing the annihilation of General John French's British Expeditionary Force and the subsequent success of the Marne offensive in 1914 and later in supporting the battles of Messines Ridge, Cambrai, and Amiens.[14] Intercept at sea played an important role in enforcing the blockade of Germany and warned Admiral John Jellicoe of the sailing of the German High Seas Fleet prior to the Battle of Jutland.[15] Tactical intercept also impacted the air campaign, providing early warning for the British of German bombing raids through the interception of ground-to-air radio transmissions and the employment of early direction-finding technology.

Britain's Strategic Information War

By 1914, Britain had recognized that information could and subsequently would be used to defeat Germany. The seeds for this recognition had been sown in Britain's experiences in strategically controlling the flow of information and manipulation of its content during the Boer War.[16] In 1911, discussions held by the Committee on Imperial Defence formalized these seeds into a plan concerning the actions that would be taken on the outbreak of war with Germany, an event that even 3 years before the start of hostilities seemed increasingly likely.[17] Britain saw this weaponization of information as supporting its strategic aims *militarily* by disrupting Germany's ability to command its overseas forces, preventing the conduct of war on a global basis; *diplomatically* by preventing Germany from establishing alliances with other states sympathetic to its cause; and *economically* by restricting German access to global financial markets and the establishment of economic relationships with other states, hindering its ability to resource its war effort. This last aspect was particularly important regarding the enforcement of the maritime blockade that Britain and its allies imposed on Germany from 1914.[18]

Ethical implications concerning the actions taken by Britain during the 1914–1918 period were seemingly not discussed at the time. The reason for this remains unclear. One explanation can be related to the overall lack of the application of ethical consideration to the use of new technology in warfare. A second, more specifically, concerns the view taken during the period, or lack of it, to the exploitation of private information, whether that of the state or of the individual. At the outbreak of the war, Britain's only legislation concerning the interception of information related to postal intercept and was based on the proclamation of May 25, 1663.[19] Inception of the telephone (encompassing its transit through cable networks) and radio communications was not placed on the statute book until the 1921 Official Secrets Act.[20] Yet with hindsight and reference to events in the last decade—including the 2013 Edward Snowden revelations and the weaponization of

information through cyber means by state and nonstate actors to mount military, diplomatic, and economic attacks—Britain's actions would today generate ethical questions regarding access to Germany's information, its manipulation, disruption to its transmission, and the subsequent use that it was put to.[21] These are ethical issues that 100 years after the end of the war still resonate.

The All Red Line

At the center of Britain's information war was the exploitation of its own global cable and high-powered wireless network: the All Red Line. The network, whose construction began in the early 1850s with the laying of the first submarine cable across the English Channel, was extended in 1858 with the laying of the first transatlantic cable between Ireland and Newfoundland and completed in 1903 with the final link across the Pacific to America.[22] On completion, the global reach achieved by the All Red Line and the similar communications structures led Tom Standage to describe it as the "Victorian Internet."[23]

For Britain, the exploitation of its own network and those of other states contributed to its war effort in two ways—the first, by allowing it to govern its empire and maintain security through the command of its own troops and those contributed by states within the empire, and the second, and of significant importance to its conduct of information warfare, was the opportunity that it gave Britain to control the flow of all diplomatic, economic, and military telegraphic traffic between Europe and North and South America, including that of Germany. It had achieved this position through the physical destruction of Germany's own global communication network and critical nodes within it and the suppression of German traffic and that of its allies that passed over British-controlled cables and of traffic that transited cables operated by other states that Britain could access by the spring of 1916.[24] These efforts were supplemented by physical interdiction against myriad high-powered radio networks employed by states to reach the farthest corners of their territories and by the use of diplomatic

pressure on neutral states not to carry German traffic. In some cases, such pressure provided Britain access to traffic not possible through other means that it could exploit to reinforce its information war. All of this activity was euphemistically captured under the title of "censorship."[25]

Conducting Information War

On the opening night of the war, the British cable ship *Alert* severed Germany's five Atlantic cables that passed through the English Channel, cutting its secure communications links to the Americas. Six more cables running between Germany and Britain were also cut in the following weeks, further isolating Germany from its global cable network and the ability to use those of other states running through the United Kingdom. In the following months, British action turned to destroying German land-based communications facilities, the vast majority of which were based on high-power radio in Africa and the Far East. Noticeably, the destruction of one such capability prevented the Germans from accessing their own cable, running from neutral Liberia to South America. By May 1915, the German network in Africa and its ability to reach out globally through the African continent had effectively been neutralized.[26]

In the Far East, Britain's key focus was on the ground radio station located on the island of Yap. This station formed the pivotal node of Germany's communications network in the region and provided access to cable routes linking the island with Shanghai, the Dutch East Indies, and Guam, which in turn provided access to the United States.[27] Having completed these actions and those in Europe, Britain then concentrated on the elements of Germany's communication network located in neutral countries, the most important of these being in Spain, Portugal, Liberia, and the United States. These elements represented Germany's principal means of gaining access to its remaining cable networks and wireless stations. To achieve this, Britain relied initially on diplomatic pressure. Regarding the United States and Liberia, this worked well, with both states taking direct action to prevent Germany's use of its capabilities located in their territories.

However, diplomacy was unsuccessful in persuading Spain, Portugal, Brazil, and other Latin and South American states to act, leading the British government to conclude that it could not rely on individual states to comply with its request. Consequently, in the period between November 1914 and September 1915, German cables located within Spanish, Portuguese, and Brazilian sovereign territory were also severed.[28]

These actions left Germany dependent on its remaining radio stations in the Western Hemisphere, the passage of secret messages either through enemy lines, including the naval blockade that the Allies had put in place, and the support of neutral states, including Sweden, that were prepared to transmit German diplomatic messages under cover of its own diplomatic traffic. In 1916, in response to Britain's actions and the success of its information blockade, Germany began the construction of a global radio network using new technology that allowed transmissions to occur over greater distance, intending to link its high-powered radio station located at Nauen, a short distance from Berlin, with stations in Argentina, China, and Mexico, which in turn would link with sub-stations in Asia and the Americas.[29]

The attempt failed, as Britain attacked the network physically and diplomatically. With the assistance of Japan, diplomatic pressure prevented development of any new capability in China. Diplomacy was also successful in causing Argentina to take action against German construction, but only after Britain released intercepted German diplomatic traffic from its ambassador in Buenos Aires. This traffic was less than flattering about the United States, which the United States then released, resulting in a deterioration of German-Argentine relations and the dismantling of the German radio station. Mexico proved to be a more difficult case. After the failure of diplomatic approaches, Britain decided to take direct physical action to prevent Germany from establishing a communications network in Central America that would provide access to South America by conducting a clandestine attack against a newly built station in Mexico City, which operated as a regional node connecting Germany with the entire region. The neutralization of the station was achieved through the destruction of

newly developed vacuum tubes necessary for amplifying the signal from Nauen in an act of sabotage undertaken by a captain of the Royal Navy.[30]

The information blockade imposed on Germany's external communications network severely restricted its ability to act in the international arena and conduct military operations on a global basis. Diplomatically, it prevented Germany from gaining the support of other states to participate in the conflict against the Allies directly and, in enlisting their support to apply political pressure on Britain and the other Allied states, to prevent it from having to succumb to unfavorable peace treaty arrangements. Economically, it significantly strengthened the effect of Britain's naval blockade by preventing Germany from entering into economic relationships with other states and by restricting access to the international banking system, curbing its ability to generate financial resources to continue the war and preventing the purchase of supplies from outside of Europe. Militarily, Britain's actions constrained Germany from conducting warfare against the Allies globally by its inability to communicate securely with its overseas stations.[31] These outputs, achieved through the exploitation of intelligence on German intent, the control of Germany's strategic flow of information, and the exertion of influence on those states that Germany communicated with allowed Britain to achieve what would now in military doctrine be referred to as information advantage.[32]

The Zimmermann Telegram

The Zimmermann Telegram demonstrates how Britain used these three effects to significantly affect the outcome of the war by securing the entry of the United States into the conflict on the side of the Allies. In January 1917, German leadership, seeking to make a decisive move to break the deadlock of trench warfare on the Western Front and hasten the end of the war, embarked on a global campaign of unrestricted submarine warfare. Its purpose was to deny Britain the economic resources, primarily coming from the United States, necessary to continue to fight.[33] Concerned that this action would bring the United States into the war on the side of Britain,

German Foreign Minister Arthur Zimmermann attempted to mitigate this by proposing an alliance with Mexico. If the United States did enter the war on the side of the Allies and Mexico subsequently aligned itself with Germany, then it would receive Texas, New Mexico, and Arizona after the Allies had been defeated.[34] Although Zimmermann considered sending the proposal by the more secure route of long-range submarine, this proved impossible due to time constraints imposed by the military's proposed start date of the campaign, February 1, 1917. The offer to the Mexican government was therefore dispatched, ironically as it turned out, through U.S. diplomatic channels to the German ambassador in Washington, DC, for onward transmission to his counterpart in Mexico.[35] This was one of the few routes open to Germany for the passage of diplomatic traffic across the Atlantic.[36]

As a consequence of the control that Britain exerted on Germany's flow of telegraph cable traffic, the message was intercepted by Britain as it passed en route through the United Kingdom.[37] Decryption of the telegram provided Britain with significant intelligence on Germany's future intent regarding both its decision to conduct unrestricted submarine warfare and its proposed alliance with Mexico should the United States enter the war on the side of the Allies. After some deliberation in London on how this intelligence should be used, and the failure of the recommencement of the unrestricted submarine campaign to bring the United States immediately into the war, a copy of the telegram was passed by Foreign Secretary Arthur Balfour to the U.S. Ambassador in London, Walter Page. Simultaneously, to ensure the credibility of the telegram and increase pressure on President Woodrow Wilson, Balfour magnified the German threat in Mexico and the consequences that it might have for the United States by mounting what today would be categorized as "fake news."[38] In the United States, the contents of the telegram did influence President Wilson's decisionmaking and the views of elements of American society that, up until then, had been isolationist, but only after its publication in March 1917. While it was not the *sole* reason for America's entry into the war, the principal one being

the indiscriminate sinking of U.S. merchant ships, the domestic political pressure that publication of the telegram caused contributed to forcing Wilson's hand into declaring war on Germany.[39] For Britain, however, it helped achieve its intended effect.

Information War Today

Moving forward 100 years and acknowledging the development of technology during this period, the description of the ways and means of Britain's information war mirrors closely the media headlines of today concerning the actions of states in cyberspace. Events are frequently framed through the language of conflict that describes a cyber war between states in which they seek to achieve their strategic intent through the control and exploitation of information. These events are manifested in the illegal acquisition of technology by China and Iran in pursuit of economic and military parity with their Western opponents, the theft of financial resources by North Korea and organized criminal groups (the latter of which now have capabilities once only the preserve of states), and the manipulation of news reporting through social media by Russia that has heralded the advent of fake news.[40]

Analysis of these information wars identifies five shared activities that present ethical challenges. In reflecting on these challenges, continued reference to the phrase *information war* as opposed to that frequently employed today—*cyber war*. The rationale is simple. At the center of the discussion sits the resource of information. Its control, exploitation, and use to influence the actions of a state are important, not the ways and means through which these effects are achieved, whether these are the analog measures employed in the First World War or the digital capabilities of today.

The first challenge is that information war conducted at the strategic level is a geographically boundless war that pays no adherence to national boundaries and the sovereignty of the states that they belong to. Britain's actions from 1914 onward showed that this boundless nature allowed it to deliver effects that encircled the globe from the Far East and across the African continent before extending to the Americas. This global action

mirrored the flow of information that they sought to prevent, to denude Germany from external communication, significantly reducing its ability to exercise its military, economic, or diplomatic power. Today, conceptually similar activities by states are undertaken to provide obstacles to a state's use of cyberspace and the Internet, including the prevention of information flow by distributed denial-of-service attack as experienced by Estonia in 2007 and South Georgia in 2008, undertaken from within Russia, being the digital equivalent of cutting physical cables to prevent external communications and internal system operability.[41] The theft of data belonging to Sony Pictures undertaken from within North Korea, with the purpose of influencing Sony and the U.S. Government, is reminiscent of the use of the Zimmermann Telegram in Mexico.[42] In each of these cases, the attacks were unconstrained by geographical distance and matters of state sovereignty.

The second challenge relates to the proposition that information war does not represent a single battle or engagement that can be bounded by time or traditional constraints of war regarding declaration and cessation. Rather, it is a continuous campaign that occurs beyond the duration of conflict. For Britain, its information war began 3 years prior to the official declaration of the conflict in regard to planning and generating capability, lasted throughout the war, and continued beyond the signing of the Armistice in 1918.[43] It consisted of short-term skirmishes that witnessed the cutting of cables, the physical destruction of communication structures, and the interception of telegraph and radio transmissions, to long-term diplomatic engagements with neutral states undertaken with the aim of denying Germany their support as conduits through which it could communicate in support of its war effort. Today, this notion of information war is reflected in the constant competition between states, and increasingly nonstate actors, in cyberspace as they seek to use the opportunities that this newly emerged domain has to offer. For the states involved, competition results in their being in a state of "persistent engagement," directly through the physical destruction of information or the systems on which it transits or indirectly through its manipulation and exploitation.[44]

The short-term information skirmishes of the 21st century have become those of the hack to exfiltrate data, information, or financial assets. Three prominent examples are the 2015 theft of the personal security records of 21.5 million individuals believed to have been undertaken by Chinese-affiliated hackers; the theft of $1 million by North Korea–based criminals from the central bank of Bangladesh; and the 2017 ransomware attack, subsequently attributed to Russian cyber criminals, that caused major disturbance to the operation of elements of Britain's National Health Service.[45] The long-term engagement is the diplomatic initiatives that seek to establish behavioral norms in cyberspace or create partnerships between states as a means to improve their cyber security and counter the global threat posed. In the 21st-century examples, none of the states are involved in a conflict, yet the outcomes of the attacks were those traditionally seen only in the context of war.

The next challenge is that information war produces a conflict that encompasses the spectrum of national power: diplomatic, economic, and military. Britain's diplomatic efforts to influence neutral states at the strategic level not to support Germany's expansionist ambitions or, more tactically, not to provide resources to allow it to maintain or reestablish its communication network proved successful. Equally, its ability to prevent Germany's engagement with the international finance and economic markets through the lack of communications channels delivered material effects on Germany's ability to maintain its war effort, compounding the impact of the naval blockade significantly.[46] In the military sphere, Britain's strategic effect succeeded in preventing Germany from commanding its overseas garrisons and deployed units, restricting its ability to conduct a coordinated global conflict. Success allowed Britain to focus its resources almost exclusively on defeating Germany on the Western Front. The two most noticeable exceptions were the ill-fated Gallipoli campaign in 1915 and numerous skirmishes in East Africa.

Today the use of fake news to shape and proffer the foreign policies of states in their relationships with others in the international system is an

accepted aspect of international relations and the exercise of power. It was a fundamental element of the Israel/Hamas conflict, the continuing war in Ukraine, and, perhaps most prominently, its employment by Russia in the 2016 U.S. Presidential election.[47] In the economic arena, the impact of information war has been mentioned previously in relation to the theft of intellectual property by China and North Korea, but increasingly it is the activities of cyber criminals, operating as state proxy actors, blurring the distinction between state and nonstate actor boundaries, that is having the most dramatic effect.[48] For the military lever of national power, it now operates in an environment of constant aggression, whether engaged in a legally defined conflict or not. In this environment, it must protect its networks from disruption, ensure that its data are secure and validated to maintain the level of trust necessary to conduct kinetic actions effectively and legally, and guarantee that its weapons systems will function as intended when required.[49]

The penultimate challenge is found in Britain's demonstration that information war is not devoid of or divorced from events in the physical world. Britain's destruction of Germany's undersea cables and the sabotage of station nodes on its global high-powered radio network starkly illustrated that the passage of information was reliant on manmade structures that, when destroyed, had severe consequences on Germany's ability to conduct the war both within Europe and globally. One hundred years on, and despite frequent popular reference to the "virtualness" of cyberspace, its existence as a conduit for the passage of information remains dependent on a physical infrastructure in which undersea cables remain vital to its operation, alongside increasingly large and power-hungry server farms and Wi-Fi antenna networks that have replaced the high-power radio networks of the past.[50] Plotted on a map, the infrastructure network of the contemporary environment of cyberspace would bear remarkable similarity to the telegraphic and radio network existing in 1914.

The final area of challenge relates not only to the information war that was fought during World War I and those occurring today, but also to the

wider role played by technology in driving the realities of conflict—the technological determinism of war.[51] Viewed through this lens, ethics will always be playing catch up. For Britain, consideration of its information war occurred through a prism founded on ideas related to the interception and exploitation of postal letters as they transited through the country's postal system.[52] Further ethical considerations related to the technology of the telegraph and the radio that existed on the commencement of the war were absent. Although the last decade has seen consideration by Britain and an increasing number of other states of the challenges posed by the impact of the rapidly evolving digital domain, agreement on related ethical principles remains elusive. This situation is most starkly demonstrated by the challenge of fake news and its influence on the outcome of popular votes in the United States, the United Kingdom, and France.[53]

In conclusion, three comments can be drawn from the above discussion. First the scale of the weaponization of information undertaken by Britain in World War I to control Germany's ability to conduct strategic maneuver and to influence its allies or potential allies had not occurred before. While information war has always been an element of conflict, as Thucydides noted when identifying the effects of messaging and narrative during the Peloponnesian War, its *scale* in World War I was new.[54] It was a consequence of the emergence of new communications technology in the four decades prior to the start of the conflict and its continued evolution as the war progressed. This evolution outstripped the ability of the government and military decisionmakers to comprehend the ethical challenges and requirements that the new form of warfare brought. This situation continues to exist, despite the considerable efforts made in the last decade through such vehicles as the Tallinn Manual and the United Nations Group of Governmental Experts on cyber security to reach agreement on what constitutes the ethical and just use of information as a weapon.[55] The future shows little prospect for change given the positions taken on the matter by Russia, China, and a number of other states. Positions that are diametrically opposite to that of the West are a debate over information freedom or information control.

The second concluding comment is that while just war theory existed and was acknowledged before the outbreak of World War I, it proved inadequate in dealing with the advent of new technologies of war including the tank and aircraft, alongside those related to information war. In the latter case, available documentation suggests that no direct consideration was given to the weaponization of information and the ethical impacts that might be generated.

The only identified legal consideration was made through the lens of postal intercept and exploitation, as recognition of the intercept of telephone and radio communications was not placed on the statute book until the passing of the 1921 Official Secrets Act.[56] This inadequacy of just war theory continues today in the academic and military debates surrounding cyber warfare and how states engage in and respond to the evolving technology of cyberspace.

Finally, in war, states seek to exploit opportunities to the edge of existing legal, moral, and ethical boundaries in pursuit of their strategic objectives. This position was summarized by an unidentified British statesman in 1914 concerning the exploitation of information: "Few practices save cannibalism were beyond the pale for British statesman, subject to the principle that they not be caught publicly in the act."[57] Today, for some states, the adoption of an ethical approach to the weaponization of information has changed little. For others, including Great Britain and other Western states, while the need to develop appropriate ethical principles has been recognized, reaching an agreed position continues to produce the same challenges today as existed in 1914.

Notes

[1] Thomas Boghardt, *The Zimmermann Telegram: Intelligence, Diplomacy, and Americas Entry into World War I* (Washington, DC: Georgetown University Press, November 2003), 1–37.

[2] D.T. Zabecki, "Military Developments of World War I," *International Encyclopedia of the First World War*, last updated January 17, 2017, available at <https://encyclopedia.1914-1918-online.net/pdf/1914-1918-Online-military_developments_of_world_war_i-2015-05-07.pdf>.

[3] While this technology existed prior to the commencement of the First World War—for example, the first transatlantic telegraph cable was laid in 1858 and Great Britain completed its global cable network in 1903—it had not been used so deliberately and with such an impact as a means of achieving strategic outcomes prior to 1914.

[4] For a detailed discussion of the impact of the advanced information and communications technology through which the cyber domain is constructed on the outcome of future war, see Christopher Cope, "Warfare in the Fifth Domain: A Realistic Threat or a Hyperbole" (MSc thesis, Royal Holloway University of London, 2017), available at <https://intranet.royalholloway.ac.uk/isg/documents/pdf/technicalreports/2017/rhul-isg-2017-4-cope.pdf>.

[5] Jonathan Reed-Winkler, "Information Warfare in World War I," *The Journal of Military History* 73, no. 3 (July 2009), 845–867.

[6] P.M. Kennedy, "Imperial Cable Communications and Strategy, 1870–1914," *The English Historical Review* 86, no. 341 (October 1971), 728–752.

[7] John Arquilla, "Ethics and Information Warfare," in *The Changing Role of Information in Warfare*, ed. Zalmay Khalilzad, John P. White, and Andy W. Marshall (Washington, DC: RAND, 1999), 379–401; Mariarosaria Taddeo, "Information Warfare and Just War Theory," in *The Ethics of Information Warfare*, ed. Luciano Floridi and Mariarosaria Taddeo (Cham, Switzerland: Springer, 2014), 123–138.

[8] Winn Schwartau, "Ethical Conduct of Information Warfare," in *Cyberwar: Security, Strategy and Conflict in the Information Age*, ed. Alan Campen, Douglas Dearth, and Thomas Gooden (Fairfax, VA: Armed Forces Communications and Electronics Association, 1996), 243–249.

[9] It is worth noting that each of the three definitions is taken from academic works situated firmly within what their authors consider the field of ethics.

[10] Reed-Winkler, "Information Warfare in World War I"; John Ferris, "Before 'Room 40': The British Empire and Signals Intelligence, 1898–1914," *Journal of Strategic Studies* 12, no. 4 (December 1989), 431–457.

[11] John Ferris, "The British Army and Signals Intelligence in the Field During the First World War," *Intelligence and National Security* 3, no. 4 (October 1988), 23–48; James Bruce, "'A Shadowy Entity': M.I.1(b) and British Communications Intelligence, 1914–1922," *Intelligence and National Security* 32, no. 3 (March 3, 2017), 1–20.

[12] Wilhelm F. Flicke, *War Secrets in the Ether*, trans. Ray W. Pettengill (Washington, DC: National Security Agency, 1953), 7.

[13] Ferris, "The British Army and Signals Intelligence in the Field During the First World War"; Polly A. Mohs, *Military Intelligence and the Arab Revolt: The First Modern Intelligence War* (London: Routledge, 2008).

[14] Ferris, "The British Army and Signals Intelligence in the Field During the First World War."

[15] Ibid.; Reed-Winkler, "Information Warfare in World War I."

[16] Ferris, "Before 'Room 40'"; Peter Freeman, "M.I.1(b) and the Origins of British Diplomatic Cryptanalysis," *Intelligence and National Security* 22, no. 2 (August 7, 2007), 206–228.

[17] Reed-Winkler, "Information Warfare in World War I."

[18] David A. Janicki, "The British Blockade During World War I: The Weapon of Deprivation," *Inquiries Journal* 6, no. 6 (2014), 1–5, available at <www.inquiries-journal.com/a?id=899>.

[19] Government of the United Kingdom, *Interception of Communications in the United Kingdom* (London: The Stationery Office, June 21, 1999).

[20] Ibid.

[21] Glenn Greenwald, *No Place to Hide* (London: Penguin UK, 2014).

[22] P.M. Kennedy, "Imperial Cable Communications and Strategy, 1870–1914," *The English Historical Review* 86, no. 341 (October 1971), 728–752.

[23] Tom Standage, *The Victorian Internet* (New York: Bloomsbury, 2009).

[24] Freeman, "M.I.1(b) and the Origins of British Diplomatic Cryptanalysis"; Reed-Winkler, "Information Warfare in World War I."

[25] Reed-Winkler, "Information Warfare in World War I."

[26] Ibid.

[27] Ibid.

[28] Ibid.

[29] Ibid.

[30] Ibid.

[31] Ferris, "The British Army and Signals Intelligence in the Field During the

First World War"; Ferris, "Before 'Room 40'"; Freeman, "M.I.1(b) and the Origins of British Diplomatic Cryptanalysis."

[32] Phil Osborn, "Air Marshal Phil Osborn on Intelligence and Information Advantage in a Contested World," paper presented at the Royal United Services Institute for Defence and Security Studies, May 18, 2018.

[33] Boghardt, *The Zimmermann Telegram*; Tara Finn, "The Zimmermann Telegram and Room 40," History of Government blog, January 16, 2017, available at <https://history.blog.gov.uk/2017/01/16/the-zimmermann-telegram-and-room-40/>.

[34] Government Communications Headquarters (GCHQ), "Real World Impact: How GCHQ's Predecessors Contributed to the U.S. Entering World War I," January 16, 2017, available at <www.gchq.gov.uk/information/century-how-work-gchqs-predecessors-contributed-us-entering-world-war-i>; Boghardt, *The Zimmermann Telegram*.

[35] The inference of this action is that Britain was actively intercepting U.S. diplomatic traffic as it transited through the country—a practice that Boghardt suggests was not stopped until the start of World War II.

[36] GCHQ, "Real World Impact."

[37] Ibid.

[38] Ibid.; Hunt Allcott and Matthew Gentzkow, "Social Media and Fake News in the 2016 Election," *Journal of Economic Perspectives* 31, no. 2 (April 19, 2017), 211–236.

[39] Finn, "The Zimmermann Telegram and Room 40"; GCHQ, "Real World Impact."

[40] National Counterintelligence and Security Center, *Foreign Economic Espionage in Cyberspace* (Washington, DC: Office of the Director of National Intelligence, June 25, 2018); Europol, *Internet Organised Crime Threat Assessment* (The Hague: Europol, 2017); Neil MacFarquhar, "A Powerful Russian Weapon: The Spread of False Stories," *New York Times*, August 28, 2016, available at <www.nytimes.com/2016/08/29/world/europe/russia-sweden-disinformation.html>.

[41] BBC, "Estonia Hit by 'Moscow Cyber War,'" May 17, 2007, available at <http://news.bbc.co.uk/1/hi/world/europe/6665145.stm>; Dancho Danchev, "Coordinated Russia vs. Georgia Cyber Attack in Progress," *Znet.com*, August 11, 2008, available at <www.zdnet.com/article/coordinated-russia-vs-georgia-cyber-attack-in-progress/>.

[42] Travis Sharp "Theorizing Cyber Coercion: The 2014 North Korean Operation Against Sony," *Journal of Strategic Studies* 40, no. 7 (2017), 895–926.

[43] Reed-Winkler, "Information Warfare in World War I."

[44] Richard J. Harknett, "United States Cyber Command's NewVision: What It Entails and Why It Matters," Lawfare blog, March 23, 2018, available at <https://lawfareblog.com/united-states-cyber-commands-new-vision-what-it-entails-and-why-it-matters>.

[45] Brendan I. Koerner, "Inside the OPM Hack, the Cyberattack That Shocked the U.S. Government," *Wired*, October 23, 2016, available at <www.wired.com/2016/10/inside-cyberattack-shocked-us-government/>; Lucinda Shen, "North Korea Has Been Linked to the SWIFT Bank Hacks," *Fortune*, May 27, 2018, available at <http://fortune.com/2016/05/27/north-korea-swift-hack/>; Chris Graham, "NHS Cyber Attack: Everything You Need to Know About 'Biggest Ransomware' Offensive in History," *Telegraph*, May 13, 2017, available at <www.telegraph.co.uk/News/2017/05/13/nhs-Cyber-Attack-Everything-Need-Know-Biggest-Ransomware-Offensive/>.

[46] Reed-Winkler, "Information Warfare in World War I."

[47] Irina Khaldarova and Mervi Pantti, "Fake News," *Journalism Practice* 10, no. 7 (September 5, 2016), 891–901; "IDF Counters Hamas 'Fake News' About Gaza Target with Arabic-Language Video," *Times of Israel*, July 15, 2018, available at <www.timesofisrael.com/idf-counters-hamas-fake-news-with-arabic-language-video/>; Allcott and Gentzkow, "Social Media and Fake News in the 2016 Election."

[48] "2018 Global Threat Report: Blurring the Lines Between Statecraft and Tradecraft," *Crowdstrike*, March 1, 2018.

[49] Kate O'Flaherty, "Cyber Warfare: The Threat from Nation States," *Forbes*, September 3, 2018, available at <www.forbes.com/sites/kateoflahertyuk/2018/05/03/cyber-warfare-the-threat-from-nation-states/#2706342f1c78>.

[50] "Facts and Stats of World's Largest Data Centers," September 21, 2018, available at <https://storageservers.wordpress.com/2013/07/17/Facts-and-Stats-of-Worlds-Largest-Data-Centers/>; Greg Miller, "Undersea Internet Cables Are Surprisingly Vulnerable," *Wired*, October 29, 2015, available at <www.wired.com/2015/10/undersea-cable-maps/>.

[51] For a discussion on the application of technological determinism to the conduct of war, see Fernando Rey, "Weapons, Technological Determinism, and Ancient Warfare," in *New Perspectives on Ancient Warfare*, ed. Garrett G. Fagan and Matthew Trundle (Leiden, The Netherlands: Brill, 2010).

[52] Reed-Winkler, "Information Warfare in World War I."

[53] Allcott and Gentzkow, "Social Media and Fake News in the 2016 Election"; M.T. Bastos and D. Mercea, "The Brexit Botnet and User-Generated Hyperpartisan News," *Social Science Computer Review* (December 21, 2017); Noé Gaumont,

Maziyar Panahi, and David Chavalarias, "Reconstruction of the Socio-semantic Dynamics of Political Activist Twitter Networks—Method and Application to the 2017 French Presidential Election," *PLOS ONE* 13, no. 9 (September 19, 2018).

[54] Thucydides, *The History of the Peloponnesian Wars*, trans. M. Hammond (Oxford: Oxford University Press, 2009).

[55] NATO Cooperative Cyber Defence Centre of Excellence, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Brussels: NATO, February 7, 2017), available at <https://ccdcoe.org/sites/default/files/documents/CCDCOE_Tallinn_Manual_Onepager_web.pdf>; Adam Segal, "The Development of Cyber Norms at the United Nations Ends in Deadlock: Now What?" Council on Foreign Relations blog, June 29, 2017, available at <www.cfr.org/blog/development-cyber-norms-united-nations-ends-deadlock-now-what>.

[56] Government of the United Kingdom, *Interception of Communications in the United Kingdom*.

[57] John Ferris, "The Road to Bletchley Park: The British Experience with Signals Intelligence, 1892–1945," *Intelligence and National Security* 17, no. 1 (March 2002), 53–84.