ESPIONAGE IN THE DIGITAL AGE: HOW TECHNOLOGY IS IMPACTING THE RECRUITMENT AND HANDLING OF SPIES

Kathryn W. Dehlinger

TC 660HB
Plan II Honors Program
The University of Texas at Austin

May 13, 2020

Stephen B. Slick, MPP, J.D.
LBJ School of Public Affairs
Supervising Professor

Alan E. Kessler, Ph.D.
LBJ School of Public Affairs
Second Reader

ABSTRACT

Author: Kathryn (Katie) W. Dehlinger

Title: Espionage in the Digital Age: How Technology is Impacting the Recruitment and Handling of Spies

Supervising Professors: Stephen B. Slick, Dr. Alan E. Kessler

Digital technology has transformed every aspect of society. From online grocery shopping and dating platforms to parking meter apps, digitization has reshaped the world around us. This project explores technology's impact on the "world's second oldest profession": espionage.

New developments in technology have both benefited and challenged human intelligence gathering. Gone are the days where agents can easily exchange information at personal meetings or via handling officers traveling to and from foreign countries undercover. The mobile phone and ubiquitous data have made these techniques complicated. Sophisticated governments like China and Russia, along with the U.S., have employed advanced biometric technology in transportation hubs to monitor the whereabouts of suspected government officials abroad. While technology has managed to make aspects of espionage faster, cheaper, and more efficient, it has also created demand for new techniques to combat its increased breadth and capabilities.

This project analyzes the impact of technology using the agent recruitment process. The introduction considers the impact of technology on society in general and will discuss the implications for the intelligence community. The introduction also touches on the vital role of human collection and factors that motivate individuals to spy on their own country. The project is divided into sections to discuss each step of the agent recruitment cycle: spot, assess, develop, recruit, handle, and terminate. Each section employs examples to demonstrate how traditional techniques compare to the new methods of the digital age and analyzes the associated benefits and challenges of advanced technology.

Much of the research for this project consists of examples from news stories surrounding intelligence successes and failures. It also includes insights developed from informational interviews with former and current intelligence professionals who have been forced to adapt to the digital revolution and witnessed how it has transformed their profession. These conversations help identify the ways in which the intelligence community has

adapted to rapid changes in technology and what obstacles remain to be overcome to continue receiving national security information from human sources.

The conclusion considers the overall implications of the technology on the intelligence community and how, in the midst of technological disruption, the intelligence community must work to remain competitive in the international arena.

ACKNOWLEDGEMENTS

I would like to thank my supervisor, Stephen Slick, and second reader, Dr. Alan Kessler, for their expertise, guidance, and patience throughout the thesis process. Without them, I would have never been able to craft a thesis I am proud of and excited to share. Their valuable feedback and constant support enabled and propelled the successful completion of this project. I could not be more grateful. I am also indebted to the University of Texas at Austin as well as the Plan II Honors Program for such a wonderful undergraduate education that I will cherish forever.

TABLE OF CONTENTS

ESPIONAGE IN THE DIGITAL AGE: HOW TECHNOLOGY IS IMPACTING THE RECRUITMENT AND HANDLING OF SPIES

The ability of America's intelligence agencies to gather important information from spies will depend in the coming years on their ability to exploit (and defend against) high technology being developed at a rapid pace by businesses worldwide.

INTRODUCTION

U.S. presidents and lawmakers "rely on insights from the Central Intelligence Agency to help inform their foreign policy decisions" ("INTelligence: Human Intelligence"). The CIA along with 15 other government agencies comprise the United States intelligence community. Together, these agencies work to collect, analyze, and deliver intelligence to policymakers so they have the information they need to secure the nation.

Human intelligence is the intelligence discipline that relies on human sources to acquire and convey information about the plans and intentions of foreign governments. Human intelligence, also known as espionage, is often lightheartedly referred to as the "world's second oldest profession." It is the practice of using spies or spying methods to obtain information about another country without their knowledge. Throughout history, spies have been mobilized to "create political, military, and economic advantage" (Lerner).

Stealing secrets and spying on a nation's enemies dates back to ancient times. Egyptian hieroglyphics depict the use of court spies and pharaohs' efforts to identify "disloyal subjects and to locate tribes that could be conquered and enslaved" (Lerner). The Egyptians were among the first to develop poisons and toxins to assassinate enemy leaders. Greek city-states used espionage as a powerful political tool to spy on rival-states and "provide rulers with information on military strength and defenses" (Lerner). In Ancient China, philosopher Sun Tzu is celebrated for writing a treatise on military strategy titled "The Art of War" that emphasized espionage for its utility in gaining military advantage over an adversary.

No group in history relied more heavily on spying than ancient Rome. The expansive empire spied on its neighbors to assess their military strength and resources beyond the bounds of the Roman control. The Romans also "employed intelligence forces to infiltrate tribal organizations and convinced leaders to join in alliance with Rome" (Lerner). The practice of espionage became increasingly important throughout the Middle Ages and Renaissance and into the modern age.

Similarly, rebels in the French and American Revolutions relied greatly on intelligence to offset their disadvantage in conventional military strength. The Industrial Revolution transformed traditional espionage tradecraft, providing new tools for stealing secrets. The Industrial Revolution paved the way for a new kind of espionage, known as industrial espionage, defined as "the theft of business trade secrets used by a competitor to achieve a competitive advantage" (Kenton). Spies began to steal trade secrets and intellectual property to match innovation by international rivals. In 1837, the invention of the photograph "permitted agents of espionage to portray targets, documents, and other interests as they actually were" (Lerner).

Espionage was further revolutionized as transportation and communication methods improved. The invention of the telegraph allowed governments to send coded messages and to monitor communications between other countries. By the twentieth century, espionage "had evolved into a specialized, technical field" employed by a variety of states (Lerner). Shortly after the outbreak of WWII, the United States established its first centralized intelligence agency, the Office of Strategic Services, a forerunner of today's CIA. After the war, the focus of American intelligence shifted to "more research and analysis than field operations" (Lerner).

Before the disruptions of the digital revolution, human intelligence served as a unique source of intelligence information for governments. Human intelligence or HUMINT, is gathered from individuals who have either volunteered or been recruited to spy on their own countries. According to the CIA, HUMINT is collected through "clandestine acquisition of photography, documents, and other material, overt collection by people overseas, debriefing of foreign nationals and U.S. citizens who travel abroad, and official contact with foreign governments" ("INTelligence: Human Intelligence"). Human intelligence gathering is undertaken by CIA employees known as case officers. These individuals are responsible for recruiting sources, referred to as “agents,” and securing from these persons a range of foreign intelligence objectives vital to national security (“INTelligence: Human Intelligence”). Case officers are hired and trained to have a keen understanding of human nature. Persuading someone to spy on their own country is no simple task. The ability to understand people, each filled with emotion, desires, biases, and complexities, is crucial for running assets and collecting human intelligence. (“INTelligence: Human Intelligence”).

Human intelligence is uniquely valuable and is often the only way to learn the plans and intentions of a foreign government. The use of individuals to gather information needed by the president, U.S. military commanders, and senior policymakers is risky to those involved. If humans are tasked to collect information, it is for good reason, most often because there is no alternative means of acquiring it. Human intelligence can often fill in the gaps left by signals intelligence (SIGINT), open source intelligence, and geospatial intelligence.

Marc Polymeropoulos, a former CIA senior operations officer, asserts that there is “no substitute for what is in essence a human spy” (Polymeropoulos [16:15:00]). Human sources can penetrate terrorist groups to gather information about planned attacks on Americans, trade negotiations with foreign actors, or even a hidden nuclear program. A source working in the inner circle of a foreign leader can provide an understanding of the intentions of an adversarial government. This kind of information is typically beyond the scope of technical collection which makes human intelligence an invaluable method of information collection. The Directorate of Operations, the branch of the CIA responsible for human intelligence missions, works with other elements of the Agency to uncover the most detailed plans of U.S. adversaries (Polymeropoulos [16:30:00]). One feature that sets human intelligence apart from other collection disciplines, is the ability to go back and ask agents follow-up or clarifying questions (Morrell [17:04:00]). SIGINT, for example, is only as good as the individuals who interpret it. While humans can be messy and unpredictable, the interactive nature of agent handling contributes to the value of human intelligence.

DIGITAL REVOLUTION

The digital revolution began with the transition from analog to digital technology. Digital information "is recorded in binary code of combinations of the digits 0 and 1, also called bits, which represent words and images" ("Digital Technology"). Digitization "enables immense amounts of information to be compressed on small storage devices that can easily be preserved and transported" and "quickens data transmission speeds" ("Digital Technology"). As a result, digital technology has impacted every aspect of society--education, healthcare, manufacturing, mass communications--to name a few. People have never been more connected. Disruptive innovations, "such as the Internet, social media, mobile phones and apps, cloud computing, big data, e-commerce, and the consumerization of IT--have already had a transformational effect on production, services, and business processes around the world" (Bojanova 8).

Online dating apps, residential parking meters, airline booking, and food delivery are just a few examples of daily activities revolutionized by technology. Digitization has completely transformed the structure by which businesses and societies operate, yet technology continues to evolve. Researcher Irena Bojanova wrote that the "ongoing Digital Revolution and new techno-economic paradigms will challenge organizations and individuals to redefine and upgrade their systems, acquire new skills, and foster new mindsets" (8). Like all industries, the U.S. intelligence community has been uniquely affected by the forces of technology.

The digital revolution has forced "the CIA to reconsider everything from how and where it recruits officers to where it trains potential agency personnel" (McLaughlin and Dorfman). In 2015, as a response to the onslaught of digital technology, then-CIA Director John Brennan restructured the Agency. Before the change, Agency employees were assigned to one of four directorates: the Directorate of Operations (DO), responsible for espionage, the Directorate of Intelligence, responsible for analyzing and synthesizing raw information, the Directorate of Science and Technology, responsible for creating and developing spy craft technology and equipment, and the Directorate of Support, responsible for providing financial and medical services, materials and equipment, transportation, security, and managing the logistical needs for facilities abroad ("Support to Mission").

Brennan's new structure included a fifth, brand-new directorate, the Directorate of Digital Innovation. This new directorate is responsible for "the integration of our [the U.S. intelligence community's] digital and cyber capabilities" (Schwartz). The CIA website refers to the Directorate of Digital Innovation or the DDI as the "engine of creativity, integration, and rigor that the CIA needs in the digital age, ensuring that our culture, tradecraft, and knowledge management across the board are more than equal to the challenges and opportunities of the rapidly changing world in which we operate" ("Digital Innovation").

The DDI works vigorously to keep up with rapid technological advances and focuses on developing the "tools and techniques they need to excel and prevail in the cyber and big data arenas" to protect U.S. national security interests and competitiveness. The new directorate's focus on data hopes to provide the CIA with "greater insights from analytics" (Lyngaas). The partnership between the four directorates and the Directorate of Digital Innovation ensures that the Agency adapts to the new challenges of the digital era.

The DO, "strengthens national security and foreign policy objectives through the clandestine collection of human intelligence (HUMINT), and by conducting covert action as directed by the President" ("Directorate of Operations"). DO Case Officers, also known as Operations Officers, are tasked with "clandestinely spotting, assessing, developing, recruiting, and handling non-US citizens with access to foreign intelligence vital to US foreign policy and national security decision makers" ("Directorate of Operations").

Case officers, through classroom instruction and role-playing exercises, are tied to the "agent recruitment cycle." A case officer develops the skills required to spot, assess, develop, recruit, handle, and terminate agents. Each step of this cycle is important and serves to judge the targeted person's access to secret information, personality, trustworthiness, and motivation. As noted, a prospective agent must have access to valuable information and must also possess the right personality and temperament.

Conventionally, case officers would conduct each phase of the agent recruitment cycle on a face to face basis. That is, each step of the cycle, involves in-person contact and can be a long, costly, and often dangerous process for the CIA and the potential source. Personal meetings are considered the most vulnerable aspect of an agent operation. The time of physical proximity is the most vulnerable period for both the intelligence officer and the agent. Countries like "the USA, the Federal German Republic, Great Britain, Sweden, Holland " and especially Russia, use intense counterintelligence measures to conduct thorough surveillance operations which makes physical agent meetings in foreign countries extremely risky (Konovalov and Sokolov). Physical meetings are dangerous "because the intelligence officer is often under surveillance and is naturally not always successful in ensuring his own secure approach to a meeting" (Konovalov and Sokolov).

Furthermore, case officers may spend months or even years assessing and developing targets before they agree to spy for the United States. As a result, the information acquired by these sources may not be timely or valuable.

However, there are new possibilities for human intelligence in the digital age. Digital technology may, in certain circumstances, eliminate the need for physical meetings between case officers and prospective agents. While technology has created new challenges for government officials charged with protecting national security information, fully leveraging technology in the agent recruitment process will ultimately increase the effectiveness and security of espionage by CIA and other U.S. IC agencies with a HUMINT mission.

AGENT RECRUITMENT CYCLE

SPOT

The agent recruitment cycle begins when individuals, most often foreign nationals, are "spotted" or identified based on their ability to answer the most urgent questions of U.S. intelligence analysts or policymakers. These individuals must have some kind of access to information regarding foreign countries or non-state adversaries. For instance, if a government needed information about North Korean nuclear capabilities, it would be vital to identify or “spot” someone who works in a nuclear facility there. Traditionally, these employees would be identified through surveillance, stolen documents, or other agents. Finding potential agents may require knowing who enters and leaves the facility each day. Potential agents are targeted through already mobilized human sources, or through stolen physical information, such as phone books, employee indexes, or residential addresses.

An existing source, known as an access agent, may have contacts in the targeted community or may be recruited to frequent local bars in an attempt to find out about the personal and professional lives of the residents in the community, in the hopes of identifying somebody who has access to desired information. For instance, he or she may monitor employees entering and exiting a military facility every day. Spotting potential agents can be time consuming and costly, as success is not guaranteed.

Using the traditional approach, intelligence officers have a few options: (1) agents can meet with a representative who has “entered the country without having aroused the suspicion of authorities;” (2) agents and intelligence officers can arrange meetings in a neutral third country with plausible cover stories to “explain their simultaneous arrival;” and (3) to conduct a physical meeting on US territory with a good cover story for the visiting agent (Konovalov and Sokolov).

While these options can improve the safety of a physical meeting, there is no guarantee that intelligence officers and agents will evade detection. There is always some degree of risk involved in human espionage, particularly when the case officer and his or her agent is in the same location at the same time.

Online social and professional profiles have made the process of spotting potential agents considerably easier, faster, and most importantly, safer. In the digital age, operations officers can screen open source social media profiles to identify targets while avoiding time-consuming, costly and potentially dangerous surveillance or access agent operations.

Furthermore, a case officer (or targeting officer) is not limited to open sources to find who works at a suspect facility and has access to secrets. The U.S. intelligence community can hack into a firm's databases, payroll records, phone records and listings, parking assignments, etc., to find out the name of people working there.

This technology is equally available to foreign intelligence services seeking to collect U.S. secrets. For example, Chinese intelligence officers use LinkedIn to identify potential foreign recruits (Lee). The Chinese intelligence service enlists individuals known as “spotters” who search for “potential targets, then hand them off to another intelligence officer for further assessment” (Graff). These spotters are typically “friendly officials at think tanks, universities, or corporations” (Graff). These individuals do not carry out the recruitment process themselves. They are “considered too valuable to make a recruitment approach directly,” in other words, they are big wigs at large corporations who operate under “deep cover” (Graff).

According to the director of the National Counterintelligence and Security Center, William E. Evanina, “it’s more efficient to sit behind a computer in China and send out friend requests to thousands of targets using fake profiles” than “dispatching spies to the U.S. to recruit a single target” (E. Wong). In May 2019, former employee of the CIA and DIA, Kevin Mallory was sentenced to 20 years in prison for espionage against the U.S. that began with a LinkedIn message from a Chinese intelligence official (E. Wong). LinkedIn, Evanina describes, is “the ultimate playground for collection” as the Chinese are “contacting thousands of people at a time.” Not only are foreign recruiters after classified political information, they are interested in the collection of corporate trade secrets, intellectual property, and other research (E. Wong).

The same is true for the U.S. intelligence community. Through digitization, the spotting process is made more efficient, less time consuming and lowers the overall cost. With a click of a mouse, safe inside the four walls of the CIA headquarters in Langley, Virginia, an operations officer can send feelers out to masses of potential agents to 1) increase spotting efficacy and 2) improve operational safety.

The Kevin Mallory example highlights the important consequences of digital age technology. While technology has the potential to increase the efficacy of the spotting process, the digital revolution also broadens the susceptibility to targeting from foreign intelligence services. The Federal Bureau of Investigation announced, “that anyone who publicly identified themselves as a government official was at risk for being contacted by foreign spies” (Batt). LinkedIn is an especially vulnerable platform because it has over 645 million users who are employment recruiters, headhunters, individuals who are employed and unemployed persons seeking new opportunities. Some public officials on the platform disclose their security clearances in the hope of improving their appeal and employment opportunities which, in turn, makes these individuals prime targets (E. Wong). Kevin Mallory, the former IC officer, was targeted and persuaded to spy for an adversary via social media.

In another case, former Obama senior foreign policy official, in the months after leaving his government job and visiting China, received a LinkedIn message from an employee of a company called R&C Capital identified as “Robinson Zhang.” His message read: “I’m quite impressed by your CV and think you may be right for some opportunities, which are all well paid.” The targeter offered the individual an all-expense paid trip to

China. The official, unsure about the legitimacy of the company, requested a website link to validate the Zhang's claims. The website, he later acknowledged, looked like "something he made up on the fly" (E. Wong). The company did not exist in the location listed as the address and was not registered in the Hong Kong corporate database (E. Wong).

The U.S. is not the only victim of Chinese phishing for potential agents. German and French intelligence organizations believe that over 10,000 German and 4,000 French citizens were targeted via LinkedIn by Chinese intelligence agents. In addition to leveraging the reach of technology, the US intelligence community must focus on its counterintelligence capabilities to thwart foreign influence and safeguard national security.

Employees of the CIA are instructed to be discrete on their social media accounts. They obviously cannot list the name of their employer and are told not to tag coworkers in their Facebook photos. Former CIA Deputy Director David Cohen explained that "we [the CIA] must find ways to protect our officers who increasingly have a digital footprint from birth" (Ewing).

Intelligence officials have expressed frustration with social media and generational norms. New recruits to the CIA, "particularly those born in the age of social media, ha[ve] become more difficult...with the Agency lacking clearly defined policies for social media use" (McLaughlin and Dorfman). One former Agency official claimed that the "CIA has adopted the position of 'we're not going to help you, but you better not do it wrong" (Pagliery). Until recently, the Agency advised employees of the social media generation to delete their online profiles altogether. This position has since changed because "such behavior could be seen as suspicious" in its own right (McLaughlin and Dorfman). The U.S. intelligence community currently struggles to find ways to protect their employees from being digitally linked to the IC.

The Internet has become a particularly effective spotting tool for recruiters of Al Qaeda and the Islamic State. In her *New York Times* podcast "Caliphate," Rukmini Callimachi interviewed Jesse Morton, an American recruit to Al Qaeda, who became "one of the most prolific recruiters for the group online" (Callimachi [15:45:00]). When asked how he recruits young jihadists, he explained that he spots individuals that "express interest through email" or "are consistently logging into your conversation" (Callimachi [16:00:00]). These individuals are drawn into radical propaganda--baited with media graphics, videos, speeches, and textual information. Those individuals who are consistently joining such conversations online and engaging with the propaganda are pursued to join the jihad and act on behalf of the Islamic State.

Social media has the potential to change indelibly the spotting phase in the agent recruitment cycle. By enlisting technology, spotters can quickly and safely identify potential targets with access to desired information. Social media gives spotters the ability to contact numerous individuals at one time and also conceal their true identities and aims. Technology has expanded the capabilities of intelligence officers in their search for foreign assets to provide information to protect national security. At the same time, however, the IC must focus on its counterintelligence practices to thwart foreign spotting activities among U.S. officials.

ASSESS

After a target with access to secrets is identified, the next step of the agent acquisition cycle is to assess the targeted person. These targets are assessed to determine if they may be ultimately willing to spy and if their personality and personal traits are suitable for this role. Case officers determine "whether the spotted individuals have the placement and access to provide desired information" and determine the "motivations, vulnerabilities, and suitability" of the particular target (Burkett 13). Either before or during this phase in the cycle, personal contact with the target agent is customarily established to begin building personal relationship. This relationship and a plausible basis for continuing contact helps case officers carry on assessing the target to "explore whether they will be responsive to initial tasking for intelligence information" (Burkett 13).

Case officers often travel to professional conferences or diplomatic events to initiate contact with a recruitment target. Case officers may adopt cover positions and present themselves as diplomats or citizens of a third country. When an officer assumes the identity as a citizen of a third country, this approach is known as a "false flag." In false flag operations, "actions are attributed to entities other than the ones actually conducting them" (Petkus 115). The personal contact and direct assessment often determine whether a particular individual might make a good spy. Meanwhile, case officers "explore exploitable weakness which may be used as a lever against a recruit" ("Foreign Intelligence"). These vulnerabilities may include drug and alcohol abuse, financial troubles or even an illness in the family ("Foreign Intelligence").

Case officers are not looking for well-adjusted people. Asking someone to spy is not a normal request. The targeted individual must demonstrate vulnerable traits or motivations that would compel them to consider accepting such a risky offer. Research confirms that individuals agree to spy for a number of reasons. In her article, "Why Spy? The Psychology of Espionage," CIA psychologist Ursula Wilder identified three main conditions for a person's willingness to spy: "(1) dysfunctions in the personality; (2) a state of crisis; and (3) ease of opportunity" (20). Individuals who spy often demonstrate thrill-seeking characteristics as well as lack a sense of responsibility and are often in search of power and control. Spies regard their behavior as a last resort or the only logical solution to a given state of crisis or distress. Ease of opportunity is also an important factor. Individuals must have ready access to the means to address their immediate crisis. The case officer offers this opportunity.

The combination of these conditions creates the perfect agent candidate. Wilder explains that individuals with personality disorders tend to find themselves wrapped up in life crises which eventually lead to relationship, family and financial troubles. These "personal crises will, in turn, further stress and magnify problematic traits" (Wilder 21). Case officers will then "insinuate themselves into the situation and find ways to exacerbate personal crisis" (Wilder 21). Individuals with a motive to spy, the right personality and access to desired information are excellent candidates for agent recruitment.

In 1985, Aldrich Ames, chief of the counterintelligence branch in CIA's Soviet and East European Division, notably one of the most notorious spies in history, sold the names of two agents reporting to the KGB in the United States. He was given $50,000 for this information. He continued to provide information to Soviet intelligence officers about the CIA and its operations in Moscow. Later that year, he received a $2 million-dollar wedding gift from the KGB for his services. To avoid raising suspicions about his new-found wealth, the KGB held much of this money "in escrow" for Ames's future use. His relationship with the Soviets continued for nine years including assignments in Rome and CIA Headquarters in Virginia. Ames was eventually unmasked and arrested in 1994.

When asked to explain his motive for betraying his country, Ames responded “money--money was the motivation” (Weiner). He claims that he did not believe his actions to be “affecting the security of this country [the United States] and the safety of its people.” He went on to claim that “very few have sold secrets to the KGB...because many of them would have found--there were a lot of barriers in the way” (Weiner). As chief of SE Division’s counterintelligence branch with the job of helping run Soviet agents worldwide, Ames was perfectly positioned to steal and sell secrets to the KGB. A painful divorce, financial troubles and ease of opportunity paved the way for Aldrich Ames to compromise the identities of many US assets in the Soviet Union and cement his reputation as one of the most damaging spies in U.S. history.

Digitization has created new techniques for agent assessment. Instead of meeting potential targets face to face, social media, online chat rooms and instant messaging enable case officers to assess potential agents virtually via the Internet. A case officer can learn valuable assessment information about a potential agent in a matter of minutes online, a process that may have taken many years to learn through face-to-face contacts. Through platforms like Facebook, Instagram, Twitter, and LinkedIn, case officers can quickly discover an individual's interests and hobbies, personal and professional networks, worldview, personality, as well as family and relationship status. Using only open source media--or information gained by hacking into a target’s phone or personal computer, intelligence officers can judge an individual's financial situation, emotional stability and suitability to spy.

For instance, social media posts may reveal that a target has a deep distain for the United States which may lead to unsuccessful agent recruitment. This type of assessment information might cause the operation to move forward under a false flag. As previously mentioned, false flag operation occurs when a case officer intentionally pretends to work for a different country, company or group to misdirect a potential agent about one's loyalties.

However, the target's online activity may also inform a case officer of a family member who needs treatment for an illness. As a result, the case officer may be able offer medication in exchange for information. Through friendships, photos, status updates, and connections, intelligence officers can unearth the daily routines and interactions of a target individual. These findings help case officers understand the overall personal and professional life of a target and provide insight for deepening a relationship with this individual.

Internet users tend to be less guarded on social media and often demonstrate a misguided sense of privacy online. According to a *New York Times* study about the psychology of online sharing, 68% of people share personal information online to "give people a better sense of who they are and what they care about" ("The Psychology of Sharing"). As a result, online social media profiles give intelligence officers a perfect tool to efficiently and anonymously assess potential agents.

New technical capabilities also enable more extreme and detailed digital surveillance. For deeper insights, intelligence services may hack an individual's computer or cell phone to analyze search histories, email correspondence, digital documents and other private information. Today, computer users frequently set up remote desktops to access computer programs and files mobile devices. Skilled CIA hackers, when pursuing lawful foreign targets, can remotely infiltrate computer desktops and mobile devices of potential sources to aid in the assessment process.

The Internet has not only eliminated the need for face to face contact but can create an online virtual dialogue between recruiters and potential targets. The Islamic State, as previously mentioned, releases immense amounts of propaganda online for young people to read, watch, and experience. In the *New York Times* podcast titled "Caliphate" Rukmini Callimachi interviewed a former jihadist Abu Huyzafah about his recruitment to ISIS.

For ISIS, the spotting and assessment stages are combined. Huyzafah, for example, was a Muslim immigrant from Pakistan living in Canada. He was a seemingly normal kid from a middle-class background who loved *Star Wars*. His family never experienced any sort of religious discrimination. However, Huyzafah wanted "something bigger… not something simple and boring" (Callimachi [03:35:00]). As a young Muslim kid growing up in the middle of the U.S. war on terror and the digital age, Huyzafah took to MySpace in search of identity and information about the Taliban and Al Qaeda. Huyzafah eventually finds himself in “forums, in chat rooms, where Al Qaeda and later ISIS recruiters are lurking” meanwhile listening to the lectures of Anwar al-Awlaki, a charismatic Islamic religious leader and proponent of violence (Callimachi [09:25:00]).

Huzayfah “followed a bunch of their [ISIS recruiters] pages on Tumblr” and even “tried to contact them on Facebook " and Instagram (Callimachi [14:05:00]). He eventually developed relationships with ISIS recruiters online. They answered his questions about the basis for suicide bombings, and killings, with sound religious justifications. Most importantly, he felt heard and accepted. Callamachi described this process as ISIS recruiters “reach[ing] through the internet” to “hold their hand as they started down the funnel of radicalization” ([13:40:00]).

In essence, ISIS recruiters operating from safe havens in Syria and Libya, use social media as platform to connect with and develop jihadist recruits. Callamachi describes the “tens of thousands of people like Huzayfah who are circling these internet watering holes” (Callimachi [14:05:00]). The internet and social media platforms provide both information and a deep sense of community to young, lost individuals. Individuals like Huzayfah buy into the radical ideology while ISIS recruiters stand ready in online chatrooms to spot and assess vulnerable individuals to join the jihad.

DEVELOP

After a target with access to secrets is assessed or deemed suitable to spy the development process begins. In an interview at Harvard, former CIA deputy director for operations, Michael Sulick, described the development process as “another word for cultivating personal relationships” (3). This involves spending time with a target, exploring shared interests, communicating frequently and getting to know one another. This relationship is established based on trust and indebtedness.

The “principle of reciprocation” is vital during this stage. In his article, “An Alternative Framework for Agent Recruitment,” CIA historian Randy Burkett asserted that “one of the easiest ways for a case officer to initiate and develop a relationship with a potential agent is to fill some small need the agent has revealed” (14). These small gestures may involve obtaining scarce medicine for a family member, helping with a visa application, finding employment opportunities, a kind gesture, or offering sincere personal advice. Any favor or act of kindness creates in the recipient a sense of obligation. Burkett suggests that in “the agent recruitment process, small commitments in the development phase… can grow into full recruitments” (16). In any case, reciprocation is successful when a target feels indebted to a case officer and paves the way for a case officer to ask for something in return.

Persuading an individual to betray his or her own country and spy for you requires trust. Sulick addresses the question of using blackmail to coerce individuals to give up secrets. He asserts that "blackmail doesn't work practically" (3). Case officers want agents who will freely cooperate. If someone is being forced to commit espionage, he or she "will give you as little information as possible and be as uncooperative as possible" (Sulick 3). This is not the kind of individual who can provide national security information to the U.S.

During the development phase, "case officers will often demonstrate their authority by indicating they have special positions or powers beyond whatever jobs they claim to hold in the US government or business" (Burkett 14). For instance, case officers may claim the ability to "richly reward consultants," setting the foundation for future monetary compensation (Burkett 14). The impulse to reciprocate and a case officer's aura of authority give foreign targets the impression that case officers are credible. During development, case officers set the conditions before they formally ask a target to spy.

Before the digital revolution, the development phase, like the others, was conducted face to face. Furthermore, the development stage was similarly time consuming, costly and risky because it required frequent point of contact that may attract the attention of interested security services. Case officers could devote years to socializing, spending time with one another's families, and establishing shared interests to build a personal relationship with a potential agent. However, the internet has provided people with many tools to find community, shared interests and build meaningful relationships online.

In the digital age, the concept of an “internet relationship” is a widely accepted phenomenon. Wikipedia defines an internet relationship as a relationship between two people who have met online, and in many cases know each other only via the internet. According to *Statista*, in 2019, the average amount of time a person spends on social media per day is 144 minutes (Clement). That is, about two and half hours of reading material posted on social media outlets like Facebook and Instagram, communicating with other online users via Twitter or WhatsApp, and engaging in online exchanges.

People access dating sites like Bumble and Tinder to connect with others seeking a partner. Similarly, others use blog sites like Tumblr to share interests. Facebook groups are popular for fandoms and social movements. For example, on Netflix’s new docuseries “Don't F*ck with Cats: Hunting an Internet Killer” a team of cat lovers and animal rights activists were enraged by a video of an individual brutally murdering a cat. They formed a Facebook group to find and stop the perpetrator whose violence escalated to the murder to human beings. Two key individuals, using aliases “John Green” and “Baudi Moovan” were the leaders of the group. Through teamwork and persistence, the group identified the dangerous individual and saved the lives of potential victims. Group members, who had never met face to face, developed strong online relationships based on a shared cause. They are still virtual friends today.

In Rukmini Callamachi's *New York Times* podcast, "Caliphate," Huzayfah believed in and felt loyal to the Islamic State and its ideology. Through the countless conversations with online recruiters, Huzayfah developed strong personal relationships and deepened his belief in the ideology of the Islamic State. Huzayfah eventually reached out to active online ISIS recruiters to initiate his journey to jihad. According to Huzayfah, the recruiters "had everything planned out," all of the logistics and all he "had to do was just take the step." ISIS recruiters basically had a "do-it yourself guide" with information on everything from plane tickets, to safe houses to trusted smugglers. Huzayfah arranged his travel and a cover story for his parents and continued on his journey to jihad.

While he was enlisted as a young jihadist martyr rather than a foreign agent, technology enabled ISIS recruiters to successfully persuade Huzayfah to join the Islamic State. ISIS recruiters working in Syria and Libya managed to convince Huzayfah, who was living a normal life in Canada, to travel halfway around the world and join their cause. While face to face interactions have the potential to deepen human connection, technology can provide a substitute for intelligence recruiters to successfully spot, assess and develop targets. Huzayfah's story demonstrates the notion that human relationships can be built with the assistance of technology. This tool, if leveraged effectively, has the potential to increase the safety, speed and efficacy of agent recruitment.

RECRUIT

Successful agent recruitment is the ultimate objective. The case officer either formally or informally asks the individual to spy on their own country and pass secrets to the U.S. If someone is formally asked to spy, a U.S. case officer will likely reveal that he or she is from the CIA or another IC agency and would like the individual to provide information. This is a classic example of direct recruitment.

Recruitment requests "should make clear to potential agents that they are being presented with a fleeting opportunity to act on statements they have made concerning their beliefs, goals, and ideals" during the development phase (Burkett 15). Case officers work to create "a sense of urgency" and emphasize "that they have superiors who need proof of their agents' utility or they will order relationships ended" (Burkett 16). If a case officer developed the relationship under a false flag, he or she may request government or even corporate insights to help Canada, for instance, stand up to the U.S. The success of the recruitment process is contingent on accurate assessment and effective relationship building during earlier stages in the cycle.

Since the rise of ISIS, cities around the world have fallen victim to attacks by individuals motivated by the ideals of these religious extremists. Attacks by radical individuals are referred to as acts of lone-wolf terrorism. These lone actors are “inspired by the recruitment videos and hashtag campaigns delivered via social media by the Islamic State and other terrorist groups” (Easterly and Geltzer). These individuals, however, are not given direct attack instructions from the group’s leaders. Instead, these individuals “select their own targets, choose their own weapons, determine their own timing, and increasingly, record their own press releases” (Easterly and Geltzer). Individuals swear loyalty to an extremist group and acts on its behalf.

In 2016, Omar Mateen, a 29-year old, murdered 49 people and injured 53 others in a mass shooting at the Pulse nightclub in Orlando, Florida. Before the attack, Mateen posted a series of angry statements to Facebook. He was enraged by the series of bombings conducted to weaken the Islamic State in Syria and Iraq. His posts condemned the west and warned of vengeance by the Islamic State (Blinder et al.). The gunman also spoke of his loyalty to the leader of the Islamic State, Abu Bakr al-Baghdadi. In his eerie final post, he declared “in the next few days you will see attacks from the Islamic State in the USA” (Yan et al.). During the rampage, he even dialed 911 to pledge his allegiance to the extremist group.

The following year, a man named Salman Abedi set off a suicide bomb at an Ariana Grande concert in Manchester, England during the final song of her set. The attack, also claimed by the Islamic State, took the lives of 22 people and injured 116 others. This tragedy is another demonstration of the global reach of that extremist group enabled by online media.

While both these individuals acted independently, the term “lone wolf” is misleading. In addition to footage of beheadings and violence, the Islamic State shrewdly uploads content depicting evidence of great community and camaraderie as benefits of group membership. One element of this community is local, in “particular towns in Syria where foreign fighters have found new, better homes, wives, and lives” (Easterly and Geltzer). The other part of that community is global, that is, by joining ISIS and operating on the group’s behalf, “you instantly find yourself with brothers, sisters, meaning, and a place in history” via online communications (Easterly and Geltzer).

In his article, “The Virtual ‘Caliphate’: Understanding Islamic Propaganda Strategy,” Charlie Winter discusses the ways in which the Islamic States portrays this sense of brotherhood. The group frequently publishes “videos and photographic reports depicting istirāhat al-mujāhidīn” the concept of “fighters relaxing with tea and singing with each other” emphasizing the “idea of brotherhood in the caliphate” (Winter 27). As a result, lone individuals from outside the region are “no longer really alone - nor do they consider themselves to be” (Easterly and Geltzer). The Islamic State uses the internet to “build a virtual community of hundreds or thousands of sympathizers and recruits” (Easterly and Geltzer).

Creating a sense of “belonging” is no longer limited by physical distance. These “agents,” of the Islamic State are recruited and mobilized to conduct deadly attacks based on ideology delivered through social media. The success of the Islamic State in recruiting operatives through the internet presents a dangerous threat. “Agents” or martyrs of the Islamic State do not have to travel to the group's homebase in order to feel connected or to work on the group’s behalf. In essence, individuals buy into the extremist ideology and join their cause without physical contact. While this kind of “recruitment” is less direct and deliberate, it serves as a compelling example of the internet’s persuasive ability. For ISIS, the internet has removed the need for face to face contact with potential jihadists. As a result, the internet has broadened and strengthened the group’s ability to spot, assess, develop and recruit individuals to engage in jihad.

Similarly, Abu Huzayfah developed online relationships with ISIS recruiters who encouraged his belief in radical ideology and convinced him to travel to Syria to join the jihad. They rewarded his decision with the promise of brotherhood and a life of fulfillment. Huzayfah felt connected and indebted to these online recruiters, people he had never physically met. These examples demonstrate the incredible persuasive power of the internet. Intelligence officers can leverage technology to reach a wide range of individuals and can use the breadth, speed, convenience and connectivity of technology to successfully recruit individuals for espionage.

HANDLE

After a target accepts recruitment, the agent's handling begins. Handling or "running" an asset is the effective management of agents "in order to exploit his/her access to secrets" (Wippl 781). Polymeropoulos compares the development and recruitment steps to a "romance" that sets the foundation for the "highly personal, intense, and emotional" (Wilder 35) relationship between an agent and handler that blossoms into a "marriage" once handling begins (Polymeropoulos [12:50:00]). Effective handling is "designed not only to collect classified information but also to stabilize and reassure the spy in the interest of sustaining his or her capacity to commit espionage for as long as possible" (Wilder 34-35). Once an individual agrees to spy, the case officer ultimately has two responsibilities: 1) acquire the intelligence to which the asset has access and 2) keep the asset safe (Morrell [12:23:00]).

For an agent to remain safe, all communications with his or her case officer must go undetected. In order to maintain operational safety, case officers employ tradecraft techniques to evade surveillance and avoid detection by foreign intelligence services. Human intelligence collection has traditionally relied on the case officer's ability to conceal from local authorities his or her affiliation with an intelligence service. This is the concept of cover. Case officers often travel to foreign countries claiming to be employees of the U.S. embassy, diplomats, students or academics with supporting cover stories and documentation.

Two dimensions of “cover” exist in spy craft: cover for action and cover for status. Cover for status refers to an individual’s personal and professional “identity.” An individual traveling abroad as a student or diplomat, for example, justifies his or her presence in a foreign country using cover for status. Cover for action, on the other hand, explains why someone is at a particular meeting site on a certain day and time. The purpose of cover is to ensure an intelligence officer does not attract the attention of a local counterintelligence service. For instance, when U.S. case officers enter a country like China or Russia, their presence can raise red flags especially if their true identities are known to the country from unrelated activities. As a result, CIA officers need defensible cover identities to justify their international travel and work assignments.

In the first several decades of the CIA, successfully deploying case officers required “creating a plausible alias or “legend” for an undercover officer; that officer’s ability to convince anyone who cared that he was the person he said he was; and having the documents to buttress that legend” (Naylor). For example, famous CIA technicians like Antonio J. “Tony” Mendez worked as professional forgers. Mendez helped maintain upwards of 15,000 aliases at the CIA and created forged ID cards, birth certificates, school records, passports, visas and plane tickets.

Over time, the CIA increased its sophistication and built “aliases for its officers that allowed them to pretend that they were neutral [citizens of] ‘third countries’ - neither the

United States nor the country in which they were operating" with matching paper trails (Naylor). Most CIA officers work under official cover, meaning that they pretend to work as a U.S. diplomat assigned to an embassy abroad. Others work under non-official cover abroad in the private sector without the safety net of diplomatic immunity.

One compelling example of a successful operation using cover identities and disguises was the mission to exfiltrate six American diplomats sheltered by the Canadian Embassy in Tehran after the U.S. embassy was taken over in 1979 by Iranian revolutionaries. This mission inspired the film "Argo." On January 25, 1980, after opening a fictional production office in Los Angeles, Six Studios Productions, creating the career histories for the six Canadian "diplomats," and promoting a new sci-fi film on U.S. media outlets, Antonio Mendez, the inspiration for Ben Affleck's character, traveled to Tehran under Canadian alias "Kevin Cost Harkins" (Smith). Upon arrival, Mendez and his CIA colleague, Julio, spent several days coaching the diplomats on their new identities as cameramen and set designers and preparing them for their exit interrogations at Tehran's Airport. On January 28th, Mendez managed to safely smuggle the six Americans out of Tehran through the use of cover identities. His tenure with a CIA was "effectively a geopolitical theater" (Smith). He used "techniques from magicians, movie makeup artists and even the television show *Mission: Impossible*" and transformed "agents into characters with backstories, costumes, and documents that helped them evade detection and avoid capture in foreign countries" (Smith).

Today, however, even with the most creative talent, identification software has created new challenges to maintaining cover. According to Duyane Norman, former senior CIA official, “the foundations of the business of espionage have been shattered” (McLaughlin and Dorfman). In the digital age, “a cover identity that would have been almost bullet proof 20 years ago can now be unraveled in a few minutes” (Lucas). Digital histories pose a serious threat to officers’ cover legends. Foreign states have the ability to track everything from credit-card transactions and internet searches to social media postings and car rentals. These advances are a double-edged sword. The activities of officers born in the age of the internet have digital trails that undermine their cover identities while having no digital record is similarly suspicious. Instead of relying on disguises and memorized cover stories, individuals traveling undercover now must have plausible digital histories.

Emerging biometric technology has strained the ability for intelligence officers to travel in alias identities. In the 2000s, there was a “biometric explosion,” that is, an increase in fingerprint, facial recognition and iris scanning technology. Biometric technology poses a threat to officers traveling abroad with assumed cover identities. According to former acting CIA Director Michael Morrell, “facial recognition and biometrics make it very difficult to travel in alias.”

For example, Singapore “developed a database that incorporated real-time flight, customs, hotel, and taxicab data” (McLaughlin and Dorfman). Together, this information “would trigger an alert to Singaporean security systems” in the case that it “took too long for a traveler to get from the airport to a hotel in a taxi” (McLaughlin and Dorfman). If the security system was alerted, the Singaporean intelligence services would go to the hotel and monitor the suspected individuals through TVs and phones. According to an anonymous intelligence official, “you used to be able to fly into a country on one name and have meetings in another” (McLaughlin and Dorfman). CIA was forced to halt operations in Singapore due to the safety threat to case officers traveling in an alias identity.

Additionally, a new video application, owned by the Chinese government, known as TikTok, may have serious national security implications. TikTok is a social media platform where users share short videos, usually fun dances to catchy music. The app, released in 2017, has been downloaded over 100 million times in the United States and 1 billion times around the world. In 2018, TikTok was downloaded to user devices more than Facebook, Snapchat, and Instagram. The company, which spends over $3 million every day on advertising, requires new users to register with their name, email, and other personal information (Banks). Not only does the video application collect personal data, TikTok captures “close-ups of people’s faces, allowing the company to gather biometric data on its users” (Q. Wong) and uses AI algorithms to “record and track users’ faces” (Banks).

Biometric technology has already increased the difficulty of traveling under alias abroad. In late 2018, investigations revealed that TikTok stored much of its user data within China. As a result, “data localization laws grant the Chinese government unrestrained access to data stored in its territory,” potentially jeopardizing the privacy and personal information of U.S. citizens and other individuals all over the world (Banks). Today, the company claims that its data is stored in the U.S., however, many fear that “data sharing with Chinese intelligence services is still possible” (Banks). The ability to record and track users’ faces is problematic for the U.S. intelligence community. TikTok’s immense user base provides an abundance of personal data to the Chinese intelligence services that can undermine the safety of U.S. human intelligence missions and citizens traveling abroad.

The “dead drop” of “dead letter box” has historically been one of the most important techniques for case officers and agents to communicate securely. A dead drop can be defined as a “method of spycraft used to pass items or information between two individuals using a secret location, thus not requiring them to meet directly, so as to maintain operational security” (Greenberg). During this coordinated exchange between two individuals, typically an asset and a case officer, one party leaves a physical object, either a piece of paper, equipment, cash, or some other item in a designated location. After a period of time, the other party will come to retrieve the “cache” at the site. Infamous spies, like former FBI special agent Robert Hanssen, used dead drops to communicate with their Russian handlers. One of Hanssen’s favored dead drop locations was under a footbridge in Foxstone Part in Vienna, Virginia. Here, Hanssen would hide computer disks and documents in a bag of trash. He would then stick a piece of tape on a park sign to notify his case officer to retrieve his cache.

Hanssen was arrested in this same park while placing a package containing classified information for his Russian handlers (“Robert Hanssen”). The *New York Times* senior director of information security, Runa Sandvik, describes the dead drop as “a way to control exactly how and when a package is delivered and who has the ability to pick it up, to control more of the variables and never have to meet in person” (Greenberg). While the dead drop has been an effective tool for communications between agents and handlers, the digital revolution has started to change the rules of this game. New technological developments have made detection easier and security increasingly difficult.

The mobile phone, an excellent “tracking beacon,” presents new challenges for traditional tradecraft techniques like the dead drop (Lucas). For instance, Russian counterintelligence services can easily monitor the movements of mobile phones in Moscow. As a result, the intelligence service could match the movements of individuals based on a “phone signal that pings in the same location in the same time window” as another mobile device near a suspected dead-drop location and effectively uncover the identities foreign assets and U.S. officials (Lucas). The obvious solution would be to not carry a cell phone, yet in the digital world, it would be suspicious for an individual to live without a mobile device.

Furthermore, counterintelligence services use CCTV and other surveillance methods to track suspected intelligence officers. For example, Xuehua “Edward” Peng was arrested by the FBI as an illegal foreign agent working on behalf of China’s Ministry of State Security (MSS). From 2015 and 2018, Peng used dead drops to exchange information with a double agent run by the FBI. On four separate occasions, Peng was caught on camera hiring a hotel room and leaving a key for a source. He would then leave envelopes of cash in the room and retrieve an SD card from the foreign agent (Schapiro). Peng then traveled to China, presumably with the SD card, to deliver the information to MSS officials. The Peng case demonstrates safety risks of the digital age. The ubiquitous use of video technology compromised Peng’s cover and tradecraft and led to his arrest (Schapiro).

Today, one approach to cover identities is to “hide in plain sight.” An intelligence officer will “actually work as the professional engineer or businessperson that they present themselves to be” and use “true names, though they are known to their CIA counterparts by a pseudonym” (McLaughlin and Dorfman). Case officers may be provided real identification documents in an assumed identity from the Social Security Administration, the Department of Health and Human Services, and the IRS while also working with “digital companies, like commercially available ancestry databases, to alter personally identifying information, and also backdate work histories” (McLaughlin and Dorfman). Young people, growing up in the digital age, typically have significant digital histories. This presents an issue when hiring new employees at intelligence agencies. To combat the challenges of digital technology, government agencies and the private sector must cooperate with one another.

For example, in 2010, after years of surveillance and analysis, the FBI arrested Anna Chapman along with nine other Russian officers working under “deep-cover” in the United States. The case, known as Operation Ghost Stories, continued for over 10 years. The officers, known as “illegals,” worked for the Russian foreign intelligence service, known as the SVR. Over the course of the operation, the Russian “illegals” established seemingly normal lives in the U.S. They got married, had kids, bought homes, and “assimilated into American society” (“Operation Ghost Stories”). According to a statement from the FBI, “the SVR was in it for the long haul” and the “illegals were content to wait decades to obtain their objective, which was to develop sources of information in U.S. policy making circles” (“Operation Ghost Stories”). While the Russian spy ring never seriously compromised U.S. national security, they had the potential to cause great harm.

In order to communicate clandestinely, the Russian spy ring used a sophisticated method of digital tradecraft known as steganography. Steganography is defined as “the technique of hiding secret data within an ordinary, non-secret file or message in order to avoid detection” where “the secret data is then extracted at its destination” (Rouse). The spies communicated via publicly available photographs where “the pictures’ real importance was tucked inside, in encoded messages detailing secret meetings” (Calamia). The messages were encoded on the pixel level. Every digital color is a “combination of red, blue, and green--digitally represented as three numeric values.” Through “subtle changes in these numbers, the Russians hid binary code that the recipient with the right software could recombine into a message” (Calamia). The use of these encrypted messages hidden in seemingly normal online photos demonstrates new possibilities of handling agents in the digital age.

Operation Ghost Stories serves as an excellent example of sophisticated digital tradecraft. Strong commercial and proprietary encryption techniques, like steganography, have enabled case officers and foreign agents to exchange information via the internet. While the Russian spy ring used outdated steganographic technology that left traces of their communications, secure encryption eliminates the need for physical exchanges of information like the traditional “dead drop” or in-person meetings, the most dangerous and vulnerable espionage act. New tradecraft techniques tailored to the internet offer safe and reliable ways for agent handling without frequent personal meetings.

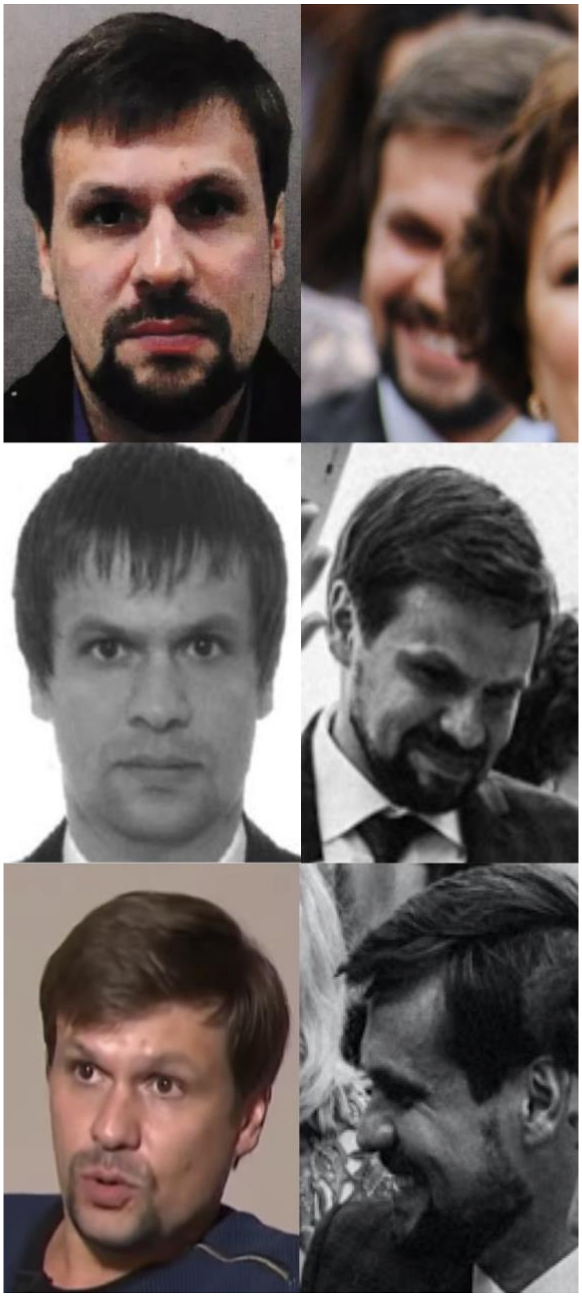
Bellingcat, a global journalism group composed of researchers, journalists, and investigators, confirmed Moscow's involvement in the poisoning of Sergei Skripal and his daughter on a park bench in Salisbury. The group relied on open sources and social media data for their investigation. The group has been successful using of publicly available information to solve suspicious cases. In 2004, Sergei Skripal, former Russian intelligence officer, was arrested by the Russian internal security service (FSB) for passing information to Britain's MI6 in the 1990s and early 2000s. He was convicted of high treason and sentenced to 13 years in prison.

In 2010, Skripal was released along with three other western agents in exchange for the ten Russian "illegals" involved in Operation Ghost Stories in a "spy swap" between the U.S., UK and Russia. After the swap, Skripal was resettled in the UK to live out the rest of his life. However, on March 4, 2018, Skripal and his daughter, Yulia, were found on a park bench in Salisbury unconscious and foaming at the mouth. The British investigation indicated that the pair were poisoned with nerve agents sprayed on the front doorknob of Skripal's Salisbury home. Most observers assumed Russian involvement in the attack, but Moscow denied the allegations.

Bellingcat, suspicious of Moscow's role, continued their investigation. Two Russians, Alexander Yevgenievich Petrov and Ruslan Timurovich Boshirov, were the prime suspects in the case. CCTV footage recorded the pair arriving in London's Gatwick

Airport and traveling from London’s Waterloo Station to Salisbury by train on two different occasions during their visit to the UK, first on March 3rd and again on March 4th, the day of the attack. The suspects claimed to be civilian tourists with no involvement in the attacks. They said they had been planning a trip to Salisbury to visit historic sites for months. However, Aeroflot’s digital passenger manifest revealed that the pair “made their initial booking--and checked in online--at 20:00 GMT (22:00 Moscow time) on March 1, 2018, the night before their short trip to London and Salisbury” (*Bellingcat* Investigation Team). Furthermore, the names Petrov and Boshirov were registered in the central Russian resident database in 2009 yet “no records exist for these two personas prior to 2009,” suggesting that the two were traveling under flimsy alias identities (*Bellingcat* Investigation Team).

Bellingcat’s analysis of open source material and photographs uncovered the real identity of Russian GRU officer Ruslan Boshirov. Investigators found photos and videos of “Boshirov,” rather, Anatoliy Chepiga, at the 2017 wedding of the daughter of Major General Andrey Vladimirovich Averynov, the commander of the Russian military intelligence service’s (GRU) military unit 29155. The ubiquitous nature of digital technology has made any sort of identity deception virtually impossible (*Bellingcat* Investigation Team).



The top-left and bottom-left photos depict “Ruslan Boshirov.” The middle-left photo is the passport image of Anatoliy Chepiga. The right columns provide images of Chepiga attending the 2017 wedding of GRU commander Major General Andrey Averynov.

Ultimately, Operation Ghost Stories demonstrates the potential of digital technology to improve the operational safety human intelligence missions. However, the breadth of the internet and open source media can undermine the security of agents. *Bellingcat's* open source investigation of the Skripal attack accentuates the ubiquity of the internet. While encryption and sophisticated digital tradecraft enables agents and handlers to communicate securely, intelligence services must also be wary of publicly available online information, digital histories, and mobile devices that may threaten operational security and agent anonymity.

MOTIVATE, COMPENSATE, TURNOVER, AND TERMINATE

The final step of the agent acquisition cycle is termination. Termination can include compensation for accumulated work, the conclusion of a secret relationship that is no longer productive or useful to the intelligence service, or the transfer of an agent to a new case officer.

For compensation, agents are conventionally rewarded in cash delivered by means of a "dead drop" of some kind. The case officer leaves money, gold or other valuables in an agreed upon location for the agent to pick up. However, during this exchange, the case officer and agent still run the risk of detection. However, new forms of electronic currency in the digital age, like Bitcoin for instance, provide a means of compensating agents that is much harder to trace. Bitcoin operates with pseudonyms. The pseudonym is the "address to which you receive your Bitcoin" ("Bitcoin Anonymity"). Each transaction from the address is stored in the blockchain that "verifies the transaction between buyer and seller" (Newby and Razmazma). Bitcoin inventor, Satoshi Nakamoto, recommends using "a new (address)...each transaction to keep them from being linked to a common owner" ("Bitcoin Anonymity"). If an individual is ever linked to that particular pseudonym, the Bitcoin transactions associated with that pseudonym are no longer anonymous. The development of cryptocurrencies offers an increased degree of privacy and anonymity when employed strategically compared to traditional methods of compensating sources.

Digitization also enables easy agent turnover. For instance, a case officer may be reassigned to a new region or division. Digital information is easily transferred to the replacement officer. The turnover may even be invisible to the agent who has never met the person who recruited him or her online. A new handling officer can simply carry out the handling relationship in the role of the recruiting case officer. Without the need for physical documents and in-person meetings, case officer and agent interactions are faster and safer.

CONCLUSION

Digital technology is profoundly changing the discipline of human intelligence gathering. New data and digitization technologies make each phase of the agent recruitment cycle safer, faster and easier. With a few clicks of a mouse, one can discover someone's relationship status, travel history, hobbies, academic background, employment status along with ideas about worldviews and political orientation. Case officers can analyze public online information to spot and assess agents from inside the walls of the CIA or a field station abroad.

Online communication platforms, chat rooms and game centers give case officers a way to develop online relationships with targeted individuals so that physical contact is no longer essential to establishing trust. A number of examples demonstrate the relationship building power of the internet. ISIS jihad recruits buy into radical ideology from online propaganda and conversations with recruiters. The world has witnessed the devastating power of online relationships as lone-wolf actors under the control of the Islamic State have terrorized nightclubs and concerts. Ultimately, the internet is a powerful tool that has created and mobilized movements, revolutions, and connected people all over the world. Intelligence agencies, at home and abroad, can benefit from the limitless reach of technology to safely, quickly and efficiently recruit and handle foreign agents.

However, the impact of technology is reciprocal. In an episode of the *Intelligence Matters* podcast, Michael Morrell, former acting director of the CIA, interviewed Glenn Gaffney, former director of Science and Technology at the CIA and currently the executive vice president of in-Q-Tel, who explained that advancing technology is “creating more and more attack surfaces” for adversaries (Gaffney [11:45:00]). The IoT as it stands for the “Internet of Things,” can also be thought of as the “Internet of Threats” (Gaffney [11:47:00]). As a result, the U.S. IC must develop an “evolving understanding of the nature of attack surfaces, the way we are being attacked and how we respond within that space” (Gaffney [12:06:00]). While digitization has the potential to increase the efficacy of the agent recruitment cycle, technology invites new challenges for the intelligence community.

The CIA has already fallen victim to these hazards. For example, in 2003, Hassan Mustafa Omar Nsar also known as Abu Omar, a Muslim cleric and alleged member of Egyptian radical movement Gama’a al-Islamiyya, a terrorist organization supported by Osama Bin Laden, was abducted outside of his home in Milan, Italy. In the 90s, after residing in Albania, Abu Omar had been expelled from that country for his role in planning an attack on an Egyptian minister. He moved first to Germany and then was granted political asylum in Italy in 2001. In Italy, he served as an imam at a radical mosque and in an Islamic cultural center visited by Islamic radicals, many of whom eventually were detained, arrested and convicted for recruiting jihadists. Abu Omar was abducted and flown to Egypt as part of an “extraordinary rendition.” He claimed that the Egyptians interrogated and tortured him. Italian police deemed this abduction a kidnapping and launched a thorough investigation into the incident.

After “tying their cell phones to a place and time at which Nasr was thrown into the van” as well as credit card, hotel and car rental information, Italian law enforcement convicted 23 Americans for the abduction (Stutser). Milan prosecutor Armando Spataro was able to identify the names of several American diplomats and CIA’s Milan base chief Robert Lady along with other CIA officers. Furthermore, a flight itinerary along with surveillance photographs of Abu Omar corroborated Lady’s involvement in the 2003 abduction. The assortment of traced phone calls as well as credit card and hotel records provided Italian investigators with the evidence, they needed to convict a number of Americans complicit in the abduction of Abu Omar. This incident embarrassed the US government and imposed political costs (Sisti).

In order to stay abreast in the digital age, the IC must employ technology in a way that seems natural while considering “all of the different ways that a would-be attacker might exploit those systems” (Gaffney [11:38:00]). As technology develops, it is important to ensure these advances “behave the way you would expect them to on the streets” (Gaffney). The IC is stocked with great talent and strong relationships with private firms that drive technological advancement. The differentiating force between “winning” on the world-wide scale is the creativity in the *application* of developing technologies. The “method of delivery” of new technology is equally as important as the technology itself (Gaffney). The merger of technology and creativity is the key to intelligence success in the digital age.

Gaffney confirms the importance of “understanding our [the US] own signatures and our behaviors” within a network when it comes to espionage. This helps decipher what is and is not normal in terms of behavior. Departing from normal patterns is suspicious and potentially compromising. Operation Ghost Stories illustrated how steganography was used effectively in agent communications for over 10 years before being discovered by the FBI. The Russian “illegals” managed to clandestinely communicate for decades through the unassuming, unseen pixels of digital photos. While technology provides new avenues and tools with which to operate and communicate, the art of espionage remains unchanged.

The ongoing coronavirus pandemic provides an interesting real-world scenario that demonstrates how human behavior adapts to changed conditions. What is normal behavior in the context of COVID-19? Most countries are under stay-at-home / shelter-in-place orders. People are expected to stay at home, only visit the grocery store or pharmacy periodically, possibly go outside for exercise, and maintain a safe social distance. In April and May of 2020, amid a global virus outbreak, this is normal behavior. On the other hand, frequently leaving home, talking to people face to face, and long drives to places other than essential businesses, is not normal behavior. This behavior is abnormal and suspicious. It is, however, the traditional signature of human intelligence activity.

Technology and creativity when paired with routine behavior, achieves the central goal of espionage--collecting valuable national security information without being compromised. At last, digital technology has the potential to streamline agent recruitment and increase the security and efficacy of the process. The U.S. IC must embrace the opportunities offered by the digital age and employ technology to enhance its fundamental understanding of human psychology.

WORKS CITED

Banks, Jim. "Rep. Jim Banks: China May Be Spying on You Through Your Phone - Urgent Investigation Needed." *Fox News*, www.foxnews.com/opinion/jim-banks-tiktok-privacy-threat. Accessed 30 Apr. 2020.

Batt, Simon. "How Foreign Spies Recruit People on Social Media." *Make Tech Easier*, 2 July 2019, www.maketecheasier.com/foreign-spies-recruit-people-social-media/. Accessed 5 Nov. 2019.

*Bellingc*at Investigation Team. "Skripal Poisoner Attended GRU Commander Family Wedding." *Bellingcat*, 14 Oct. 2019, www.bellingcat.com/news/uk-and-europe/2019/10/14/averyanov-chepiga/. Accessed 11 Apr. 2020.

Bellingcat Investigation Team. "Skripal Poisoning Suspect's Passport Data Shows Link to Security Services." *Bellingcat*, 14 Sept. 2018, www.bellingcat.com/news/uk-and-europe/2018/09/14/skripal-poisoning-suspects-passport-data-shows-link-security-services/. Accessed 12 Apr. 2020.

"Bitcoin Anonymity - Is Bitcoin Anonymous?" *Buy Bitcoin Worldwide*, www.buybitcoin worldwide.com/anonymity/. Accessed 12 Apr. 2020.

Blinder, Alan, et al. "Omar Mateen Posted to Facebook Amid Orlando Attack, Lawmaker Says." *The New York Times*, 16 July 2016, www.nytimes.com/2016/06/17/us/orlando-shooting.html. Accessed 1 Apr. 2020.

Bojanova, Irena. "The Digital Revolution: What's on the Horizon?" *IT Professional,* 8th ser., vol. 16, no. 12, 1 Jan. 2014, DOI:10.1109/MITP.2014.11. Accessed 12 May 2020.

Burkett, Randy. "An Alternative Framework for Agent Recruitment: From MICE to RASCLS." *Studies in Intelligence*, vol. 57, no. 1, Mar. 2013, pp. 1-17, www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol.-57-no.-1-a/vol.-57-no.-1-a-pdfs/Burkett-MICE%20to%20RASCALS.pdf. Accessed 11 Dec. 2019.

Calamia, Joseph. "How the Russian Spies Hid Secret Messages in Public, Online Picture." *Discover*, 1 July 2010, www.discovermagazine.com/technology/how-the-russian-spies-hid-secret-messages-in-public-online-pictures. Accessed 1 Apr. 2020.

Callimachi, Rukmini, narrator. "Recruitment." *Caliphate,* produced by Andy Mills, episode 3, The New York Times,www.nytimes.com/interactive/2018/podcasts/caliphate-isis-rukmini-callimachi.html. Accessed 5 Nov. 2019.

Clement, J. "Daily Time Spent on Social Networking by Internet Users Worldwide from 2012 to 2019." *Statista*, 26 Feb. 2020, www.statista.com/statistics/433871/daily-social-media-usage-worldwide/. Accessed 1 Apr. 2020.

Customer Insight Group. *The Psychology of Sharing: Why Do People Share Online?* New York Times, 2011. *Boston Web Designers*, www.bostonwebdesigners.net/news/why-people-share-online/. Accessed 12 Apr. 2020.

"Digital Innovation." *Central Intelligence Agency*, 13 July 2017, www.cia.gov/offices-of-cia/digital-innovation. Accessed 3 Mar. 2020.

"Digital Technology." *Encyclopedia*, 26 Mar. 2020, www.encyclopedia.com/history/dictionaries-thesauruses-pictures-and-press-releases/digital-technology. Accessed 11 Apr. 2020.

"Directorate of Operations." *Central Intelligence Agency*, 30 May. 2019, https://www.cia.gov/careers/opportunities/clandestine. Accessed 28 May. 2020.

Easterly, Jen, and Joshua Geltzer. "The Islamic State and the End of Lone Wolf Terrorism." *Foreign Policy*, 23 May 2017, foreignpolicy.com/2017/05/23/the-islamic-state-and-the-end-of-lone-wolf-terrorism/. Accessed 1 Apr. 2020.

Ewing, Philip. "Why the CIA Likes, and Dislikes, Social Media." *NPR*, 24 Feb. 2016, www.npr.org/2016/02/24/467933392/why-the-cia-likes-and-dislikes-social-media. Accessed 7 Apr. 2020.

"Foreign Intelligence Entity (FIE) Targeting and Recruitment." *Center for Development of Security Excellence*, www.cdse.edu/documents/cdse/foreign-intelligence-entity-targeting-recruitment-methodology.pdf. Accessed 7 Apr. 2020.

Gaffney, Glenn. "CIA's Former Head of Science and Tech: In New Space Race, U.S. Is Falling Behind." Interview conducted by Michael Morrell. *Intelligence Matters*, hosted by Michael Morrell, *Podcasts* app, CBS News, 11 Dec. 2018.

Gaffney, Glenn. Telephone interview. 27 Mar. 2020.

Graff, Garrett M. "China's 5 Steps for Recruiting Spies." *Wired*, 31 Nov. 2018, www.wired.com/story/china-spy-recruitment-us/. Accessed 1 Apr. 2020.

Greenberg, Andy. "Hacker Lexicon: What Is a Dead Drop?" *Wired*, 29 Nov. 2019, www.wired.com/story/what-is-dead-drop/. Accessed 1 Apr. 2020.

"INTelligence: Human Intelligence." *Central Intelligence Agency*, 30 Apr. 2013, www.cia.gov/news-information/featured-story-archive/2010-featured-story-archive/intelligence-human-intelligence.html. Accessed 10 Dec. 2019.

Kenton, Will. "Industrial Espionage." *Investopedia*, 27 Mar. 2018, www.investopedia.com/terms/i/industrial-espionage.asp. Accessed 12 Dec. 2019.

Konovalov, A. A, and V. S. Sokolov. "Meetings with Agents." *Central Intelligence Agency*, 2 July 1996, www.cia.gov/library/center-for-the-study-of-intelligence/kent-csi/vol8no2/html/v08i2a05p_0001.htm. Accessed 31 Mar. 2020.

Lee, Yee Nee. "China Is Reportedly Using LinkedIn to Recruit Spies Overseas." *CNBC*, 28 Aug. 2019, www.cnbc.com/2019/08/28/china-is-reportedly-using-linkedin-to-recruit-spies-overseas.html. Accessed 31 Mar. 2020.

Lerner, Adrienne Wilmoth. "Espionage and Intelligence, Early Historical Foundations." *Encyclopedia*, 22 Apr. 2020, www.encyclopedia.com/politics/encyclopedias-almanacs-transcripts-and-maps/espionage-and-intelligence-early-historical-foundations. Accessed 12 May 2020.

Lucas, Edward. "The Spycraft Revolution." *Foreign Policy*, foreignpolicy.com/author/edward-lucas/. Accessed 23 Oct. 2019.

Lyngaas, Sean, editor. "Inside the CIA's New Digital Directorate." *FCW*, 1 Oct. 2015, fcw.com/articles/2015/10/01/cia-digital-directorate.aspx. Accessed 12 Apr. 2020.

McLaughlin, Jenna, and Zach Dorfman. "Shattered: Inside the Secret Battle to Save America's Undercover Spies in the Digital Age." *Yahoo*, 30 Dec. 2019, news. yahoo.com/shattered-inside-the-secret-battle-to-save-americas-undercover-spies in-the-digital-age-100029026.html. Accessed 1 Apr. 2020.

Naylor, Sean D. "The CIA at 70: How Going Undercover Has Gotten Harder." *History*, 31 Aug. 2018, www.history.com/news/the-cia-at-70-how-going-undercover-has-gotten-harder. Accessed 10 Dec. 2019.

Newby, Tyler G., and Ana Razmazma. "An Untraceable Currency? Bitcoin Privacy Concerns." *Fintech Weekly*, 7 Apr. 2020, www.fintechweekly.com/magazine/articles/an-untraceable-currency-bitcoin-privacy-concerns. Accessed 12 Apr. 2020.

"Operation Ghost Stories." *FBI.gov*, 31 Oct. 2011, www.fbi.gov/news/stories/operation-ghost-stories-inside-the-russian-spy-case. Accessed 1 Apr. 2020.

Pagliery, Jose. "Want to Be a CIA Spy? Be Careful on Facebook." *CNN Money*, 13 Mar. 2015, money.cnn.com/2015/03/13/technology/security/cia-facebook-rules/index.html. Accessed 1 Apr. 2020.

Petkus, Donald A. "Ethics of Human Intelligence Operations: Of MICE and Men." *International Journal of Intelligence Ethics*, vol. 1, no. 1, Spring 2010, pp. 97-121.

Polymeropoulos, Marc. "Former Senior CIA Operations Officer Marc Polymeropolous on Recruiting and Running Spies." Interview conducted by Michael Morrell. *Intelligence Matters*, hosted by Michael Morrell, *Podcasts* app, CBS News, 16 Oct. 2019

"Robert Hanssen." *FBI.gov*, 2 Feb. 2001, www.fbi.gov/history/famous-cases/robert-hanssen. Accessed 10 Dec. 2019.

Rouse, Margaret. "Steganography." *Tech Target*, searchsecurity.techtarget.com/definition/steganography. Accessed 1 Apr. 2020

Sayler, Kelley M. "Artificial Intelligence and National Security." *Congressional Research Service*, 30 Jan. 2019, pp. 1-37, fas.org/sgp/crs/natsec/R45178.pdf. Accessed 16 Oct. 2019.

Schapiro, Rich. "California Man Charged in Elaborate Chinese Spy Operation." *NBC News*, 30 Sept. 2019, www.nbcnews.com/politics/justice-department/california-man-charged-elaborate-chinese-spy-operation-n1060446. Accessed 1 Apr. 2020.

Schwartz, Mattathias. "CIA's New 'Digital Innovation' Division Can't Seem to Keep Its Own." *The Intercept*, edited by Betsy Reed, 8 Mar. 2017, theintercept.com/2017/03/08/cias-new-digital-innovation-division-cant-seem-to-keep-its-own-secrets/. Accessed 3 Mar. 2020.

Sisti, Leo. "In Cleric's Abduction in Italy, the CIA Left All but a Calling Card." *International Consortium of Investigative Journalists*, 2 May 2012, www.icij.org/investigations/collateraldamage/clerics-abduction-italy-cia-all-left-calling-card/. Accessed 1 Apr. 2020.

Smith, Harrison. "Tony Mendez, 'Argo' Spy Who Smuggled U.S. Hostages out of Iran during Crisis, Dies at 78." *The Washington Post*, 19 Jan. 2019, www.washingtonpost.com/local/obituaries/tony-mendez-argo-spy-who-smuggled-us-hostages-out-of-iran-during-crisis-dies-at-78/2019/01/19/37e1f9a0-1c22-11e9 8813cb9dec761e73_story.html. Accessed 10 Dec. 2019.

Stutser, J. Dana. "How a CIA Officer Wanted for Kidnapping in Italy Ended up Arrested in Panama." *Foreign Policy*, The Slate Group, 18 July 2013, foreignpolicy.com/ 2013/07/18/how-a-cia-officer-wanted-for-kidnapping-in-italy-ended-up-arrested-in-panama/. Accessed 1 Apr. 2020.

Sulick, Michael G. "Seminar on Intelligence, Command, and Control." *The Program on Information Resources Policy*, Sept. 2007, pp. 1-24, www.pirp.harvard.edu. Accessed 11 May 2020.

"Support to Mission." *Central Intelligence Agency*, 30 Nov. 2016, www.cia.gov/offices-of-cia/mission-support. Accessed 3 Mar. 2020.

Weiner, Tim. "Why I Spied: Aldrich Ames." *The New York Times*, 31 July 1994, www.nytimes.com/1994/07/31/magazine/why-i-spied-aldrich-ames.html. Accessed 1 Apr. 2020.

Wilder, Ursula M. " Wilder Why Spy? The Psychology of Espionage." *Studies in Intelligence*, vol. 61, no. 2, June 2017, pp. 19-36.

Winter, Charlie. "The Virtual Caliphate: Understanding Islamic State's Propaganda Strategy." *NATO STRATCOM*, pp. 1-51, www.stratcomcoe.org/charlie-winter-virtual-caliphate-understanding-islamic-states-propaganda-strategy. Accessed 1 Apr. 2020.

Wippl, Joseph. (2019) The Art of Agent Handling, International Journal of Intelligence and CounterIntelligence, 32:4, 781-789, DOI: 10.1080/08850607.2019.1606642

Wong, Edward. "How China Uses LinkedIn to Recruit Spies." *The New York Times* [New York City], 27 Aug. 2019, www.nytimes.com/2019/08/27/world/asia/china-linkedin-spies.html. Accessed 23 Oct. 2019.

Wong, Queenie. "TikTok Accused of Secretly Gathering User Data and Sending It to China." *CNET*, 2 Dec. 2019, www.cnet.com/news/tiktok-accused-of-secretly-gathering-user-data-and-sending-it-to-china/. Accessed 2 May 2020.

Yan, Holly, et al. "Orlando Shooter Texted Wife during Attack, Source Says." *CNN*, 17 June 2016, www.cnn.com/2016/06/16/us/orlando-shooter-omar-mateen/index.html. Accessed 1 Apr. 2020.