AIR COMMAND AND STAFF COLLEGE

AIR FORCE OPERATIONS SECURITY IN THE TWENTY-FIRST CENTURY:

An Unaddressed Vulnerability

Adanto A. D’Amore, Major, USAF

WRIGHT FLYER PAPERS

Air Command and Staff College

Col Lee G. Gentile, Jr., Commandant
Col Christian Watt, Dean of Resident Programs
Lisa L. Beckenbaugh, PhD, Director of Research
Lt Col Shannon Cummins, Essay Advisor

Please send inquiries or comments to

Editor
The Wright Flyer Papers
Department of Research and Publications (ACSC/DER)
Air Command and Staff College
225 Chennault Circle, Bldg. 1402
Maxwell AFB AL 36112-6426

Tel: (334) 953-3558
Fax: (334) 953-2269

Email: acsc.der.researchorgmailbox@us.af.mil

AIR UNIVERSITY

AIR COMMAND AND STAFF COLLEGE

Air Force Operations Security in the Twenty-first Century:

An Unaddressed Vulnerability

Adanto A. D’amore, Major, USAF

Wright Flyer Paper No. 87

Air University Press
Maxwell Air Force Base, Alabama

Commandant, Air Command and Staff College
Col Lee G. Gentile, Jr.

Director, Air University Press
Dr. Paul Hoffman

Project Editor
Jeanne K. Shamburger

Illustrator
Catherine Smith

Print Specialist
Cheryl Ferrell

Air University Press
600 Chennault Circle, Building 1405
Maxwell AFB, AL 36112-6010
https://www.airuniversity.af.edu/AUPress/

Facebook:
https://facebook.com/AirUnivPress

and

Twitter: https://twitter.com/aupress

Accepted by University Press May 2022 and Published August 2022.

ISSN 2687-7260

Disclaimer

Opinions, conclusions, and recommendations expressed or implied within are solely those of the author and do not necessarily represent the views of the Department of Defense, the Department of the Air Force, the Education and Training Command, the Air University, or any other government agency. Cleared for public release: distribution unlimited.

This Wright Flyer paper and others in the series are available electronically at the AU Press website: https://airuniversity.af.edu/AUPress/Wright-Flyers/.

Contents

Foreword

It is my great pleasure to present another issue of the Wright Flyer Papers. Through this series, Air Command and Staff College presents a sampling of exemplary research produced by our resident and distance-learning students. This series has long showcased the kind of visionary thinking that drove the aspirations and activities of the earliest aviation pioneers. This year's selection of essays admirably extends that tradition. As the series title indicates, these papers aim to present cutting-edge, actionable knowledge—research that addresses some of the most complex security and defense challenges facing us today.

Recently, the Wright Flyer Papers transitioned to an exclusively electronic publication format. It is our hope that our migration from print editions to an electronic-only format will foster even greater intellectual debate among Airmen and fellow members of the profession of arms as the series reaches a growing global audience. By publishing these papers via the Air University Press website, ACSC hopes not only to reach more readers, but also to support Air Force–wide efforts to conserve resources.

Thank you for supporting the Wright Flyer Papers and our efforts to disseminate outstanding ACSC student research for the benefit of our Air Force and warfighters everywhere. We trust that what follows will stimulate thinking, invite debate, and further encourage today's air, space, and cyber warfighters in their continuing search for innovative and improved ways to defend our nation and way of life.

LEE G. GENTILE, JR.
Colonel, USAF
Commandant

Abstract

The twenty-first-century Air Force has maintained a twentieth-century operations security (OPSEC) culture, one heavily oriented toward speech and activities related to an Airman's official duties. Air Force OPSEC policy and culture insufficiently address the connected world characterized by ubiquitous data collection. This gap creates a critical vulnerability with the potential to diminish the Air Force's competitive edge in a future conflict.

This paper begins with a discussion of Air Force OPSEC culture and its failure to address the twenty-first-century information environment. It then analyzes the information environment of pervasive data collection through the lens of how commercial enterprises exploit data to target consumers. Using this construct, the paper examines how an adversary could use similar methods to conduct population-based mass surveillance and reconnaissance of the US Air Force through its personnel in garrison or on the battlefield and in advance of or during conflict.

The author proposes potential safeguards and mitigation strategies, highlighting the challenge of addressing a vulnerability that is deeply intertwined with an Airman's personal life. He further suggests adopting a framework of subjective and objective harm to reorient the Air Force's OPSEC culture. Finally, he recommends a mitigation approach based in education and training occurring throughout an Airman's career. Thus, the Air Force would be placing the same value on digital fluency as on financial literacy or physical fitness. Doing so will grow a culture of educated awareness surrounding the threat posed by ubiquitous data collection and population-based surveillance.

Introduction

Surveillance by foreign governments is typically thought of in two contexts. The first is surveillance of an individual. For example, an Airman on official travel to China might be a potential surveillance target of the Chinese state due to their affiliation with the US government.[1] The second context is an adversary tracking the location and activities of deployed US forces by either technical means, such as satellite or signal monitoring, or physical means, such as human sources reporting on troop movements. The Air Force uses operations security (OPSEC) to counter both types of adversarial surveillance.

OPSEC is intended to protect military operations by achieving *essential secrecy*, defined as the condition achieved by denying critical information and indicators to adversaries.[2] While a foreign government's surveillance of an individual Airman on an overseas temporary duty assignment is concerning from a counterintelligence perspective, its associated risk is qualitatively different than the potential harm of an adversary conducting persistent surveillance of Airmen as a collective entity. Thanks to increased access to data and rapid technological advances, our adversaries now have a low-risk opportunity to conduct surveillance and reconnaissance of our forces from afar.[3] Despite advances in our adversaries' capabilities, Air Force OPSEC policy and the culture that supports it have remained essentially unchanged in the twenty-first century.

The threat posed by computing and data gathering is being taken seriously in other sectors of the US government, most notably in the intelligence community.[4] It is understandable that intelligence agencies would be particularly concerned about this threat because the identities and activities of their personnel is meant to be clandestine. While the US Air Force may undertake covert activities in support of national policy objectives, few members of the Air Force require identity protection for their personal or professional safety; this has led to a false sense of security.

Air Force OPSEC policy and culture remain rooted in a pre-social-media, pre-digital age when our adversaries generally lacked direct access to Airmen. In the twentieth century, access to our Airmen was burdened by geography; the United States was a relative sanctuary from the enemy's prying eyes. Attempting to surveil an Air Force member required the commitment of personnel and came with considerable risk and little reward. Advances in technology have eliminated the traditional safe havens provided by geography. The internet and its attendant web of connected devices means Airmen in garrison inside the United States are no longer out of reach from enemy surveillance. In the twenty-first century, access to our forces is available through massive amounts of highly specific and individualized data created by the proliferation of sensors, social media engagement, smartphones, and other devices—obtainable to our adversaries with no physical risk. Advances in technology enable our adversaries to observe not only movement of Air Force assets such as aircraft but also movements of Airmen, individually and collectively. As a result, Airmen who would have traditionally been beyond the reach and interest of our adversaries now represent an important conduit of information they can harness and exploit.

This paper identifies a critical gap between Air Force OPSEC culture and policy and the advances in commercial computing and sensing capabilities. Airmen interact daily with a broad range of technologies that collect vast quantities of highly personalized data. While commercial enterprises exploit this data for the purpose of targeting consumers, this paper examines how an adversary could use similar methods to conduct mass surveillance of the Air Force using its members' personal online activities regardless of their geographic location. This analysis begins with the Air Force OPSEC culture and what that culture fails to address in the twenty-first-century information environment. Characterizing the environment as one of ubiquitous data collection, the paper discusses how US adversaries can use data and mass surveillance to their advantage before and during conflict and provides a framework to evaluate ways that data can harm members of the Air Force. Finally, the analysis concludes with a couple of recommendations. First, the Air Force should invest in modernizing its OPSEC culture with a focus on policy, education, and training. Second, the Air Force should adopt a mitigation approach based in education and training occurring throughout an Airman's career to create a culture of educated awareness surrounding the threat posed by ubiquitous data collection.

Key Definitions

A few key terms used in this paper are defined as follows. *Surveillance* is monitoring something of known importance.[5] *Population-level surveillance* is the ability of an adversary to monitor and track a group of individuals who share specific characteristics, such as all Air Force members or a particular demographic group, specialty, geographic location, or other subset within the Air Force. Population-level surveillance differs from mass surveillance by its ability to focus on a specific group. *Reconnaissance* varies from surveillance by using the same underlying data to identify indicators and warnings of emerging importance, such as an impending military operation.[6] The *Internet of Things* (IoT) describes the ever-expanding, largely inconspicuous sensor environment that collects real-time computerized sensory information detailing what is happening in a particular environment.[7] *Big data* is the synthesis of large quantities of diverse data sets combined in a way where the sum is greater than the parts.[8] *Artificial intelligence* (AI) is not a technology but a system that "incorporates information acquisition objectives, logical reasoning principles, and self-correction capacities" with an ultimate goal of enabling the analysis of large quantities of data and using that data to "discern a pattern to explain the current data and predict future uses."[9]

Vulnerability

While Air Force instructions describe OPSEC as a process, for the average Airman OPSEC is a culture focused on speech and actions in their work environment. US adversaries were once constrained by distance and limited available information in their ability to surveil the Air Force. Advances in technology have overcome these constraints. Today, our adversaries can monitor the Air Force, often in real time from afar, by tracking online habits using the same methods as commercial retailers. Adversaries can watch the Air Force as a whole or its individual members.

Much like watching a flock of birds or herd of cattle, when enough individuals are under observation, the movement or actions of any single member become less vital to understanding the direction the flock or herd is going. By identifying, monitoring, and indexing enough Air Force members, adversaries can create a living map of Air Force activities worldwide. With adequate data, they can use AI to enable predictive insights and forewarning, diminishing the element of surprise and undermining Air Force operations. The Air Force approach to OPSEC neglects the threat of population-level surveillance, as it was developed in an era when adversaries lacked the data and computing power necessary to harness it.

A Twentieth-Century OPSEC Culture

The Air Force culture of OPSEC is perhaps best thought of as an admonishment to protect sensitive information from disclosure, exemplified in the World War II idiom "Loose lips sink ships."[10] In World War II, this slogan and others like it were often paired with propaganda posters or even matched with retail campaigns ("Keep It Under Your Stetson"), all to reinforce the message to the public that the best way to protect sensitive information was to simply not discuss it.[11] For most Airmen, OPSEC was primarily a security function, requiring only protecting information via an office safe, locked away from prying eyes when not in use.[12] Early OPSEC campaigns oriented heavily toward speech because, unlike sensitive documents, it could not be locked in a drawer at the end of the day. Given the limitations of twentieth-century technology and information, the impediments of geography, and the lack of access our adversaries had to our forces when these campaigns were waged, a program focused on speech and document security was sufficient to obscure sensitive military information from the enemy's view. The emphasis on speech may have sufficed for the twentieth century, but the twenty-first-century information environment is filled with sensors collecting and transmitting data on our every move. Thus, a speech-oriented preventative culture is no longer enough to ensure the effective security of Air Force operations.

What Current OPSEC Culture Misses

An OPSEC culture relying on people being tight-lipped fails to appreciate how many discrete data points an Airman creates through daily life in the twenty-first century. The convergence of an abundance of data and advances in computing power coupled with improvements in AI have enabled the automation of data analysis and persistent monitoring. AI-driven surveillance is increasingly common, with 51 percent of advanced democracies using some form of it on their citizens.[13] Beyond government monitoring, data including an individual's retail purchase history, age, income, timing and location of physical activity, consumption of media, and other data points are collected in real time and sold by retailers and data brokers.[14] Commercial enterprises and social media companies use this information to generate efficiencies and revenue by targeting consumers based on population demographics and tailoring their advertising to a more receptive audience, which research shows can influence social media users.[15] Like retailers, social media companies exploit user data, typically with the goal of increasing the length and frequency of an individual's interaction on their platforms for the purposes of selling targeted advertising.

An estimated 80 percent of Americans use social media for an average of two to three hours every day.[16] Further, most Americans interact with the connected world in other ways. This interface includes using credit cards, smartphones, smart watches, computers, personal assistants (e.g., Apple's Siri or Amazon's Alexa), or any device that receives, analyzes, or disseminates data. Less visible but equally omnipresent are the sensors gathering data about our shared environment, which constitutes the IoT. The IoT creates a web of data wherein sensors share information about the environment and its occupants and then distributes that data to other networked systems. So much data is created and shared that many individuals are at best nominally aware of the level of detail they are freely revealing. The creation, sharing, and analysis of data improves user experiences, enhances safety, and creates efficiencies for people and businesses. For the military, however, this proliferation of data creates tremendous amounts of metadata that can be operationalized for predictive purposes. Metadata is so valuable to the US military that it is considered in many ways better than the content of an enemy's communications and is even used by the US for lethal targeting of enemy combatants.[17]

If the US feels confident enough in the value of metadata to conduct lethal strikes, then protecting our metadata should be a critical consideration. Author Bruce Schneier simplifies the difference between data and metadata: "data is content, and metadata is context."[18] While twentieth-century OPSEC programs did not discount the value of discrete data sets, the ability to turn a plethora of trivial data into something useful was previously elusive, particularly at a meaningful scale. AI and big data change that paradigm in that once disparate, trivial information and metadata now have context and value.

Social Media Disinformation: A Different Threat

The threat of disinformation propagated through social media has come to the forefront, largely because the US government has observed foreign actors weaponize social media to spread disinformation and false narratives.[19] The risk of social media in this respect is that an adversary could use social media to affect Air Force decision-making and behavior.[20] There is a distinct threat from the risk of an adversary using social media to target individual Airmen as a means to conduct surveillance and reconnaissance against the Air Force.

Social media interaction is generated intentionally by the user for the purpose of sharing and engagement. Billions of users engage with platforms like Facebook, Twitter, and Instagram to share hundreds of millions of posts, videos, and photographs daily, along with other interactions.[21] Social-media-enhanced surveillance merits serious consideration because rather than simply providing a channel to influence, social media can also serve as a channel to give an adversary forewarning and foreknowledge.[22]

Vast Quantities of Data

At issue is the proliferation of data coupled with the ability to analyze that data in new ways. The volume of data collection is ever increasing, doubling the "digital universe" roughly every two years.[23] In the past, limits of collection and processing capabilities meant that when a deluge of data was collected, it could not always be analyzed quickly enough to be useful in current operations and decision-making. The difficulty in collecting and processing data is rapidly diminishing thanks to increases in computing power—doubling approximately every 18 months.[24]

Major corporations value metadata because it provides insight into customer habits. They invest significant funds to acquire this data and drive future retail profits (in 2015 the value of "contextually aware computing," the metadata generated through passive sensing, was estimated to exceed $96 billion and has only increased since then).[25] The retailer Walmart has over 2.5 petabytes of data on consumer transactions, with each petabyte the equivalent of "500 billion pages of standard typed text."[26] Individual consumer data combined with other data points (available for purchase from data brokers or publicly)—including social media activity and cellphone location data—allows a company to target someone at a demographic and individual level. Walmart can combine data points as varied as a shopper's current location, the predicted weather forecast at that location, a shopper's past purchase history, and upcoming holidays to predict products a shopper might purchase.[27] Walmart is one of many retailers already conducting population-level surveillance, combining known data points with predictive computing to increase sales.

Categories of Data

Surveilling and targeting a population require structured and unstructured data.[28] Personal information such as a car loan application, credit report, or security clearance form typifies structured data. Structured data "gives names to each field in a database and defines the relationships between fields."[29] It is useful because it makes sense to humans, allowing for easy analysis.[30] Unstructured data, sometimes referred to as semi-structured data, constitutes the second type of data collected.[31] Unstructured data includes photographs, text files, social media posts, videos, PowerPoint presentations, and other information with quantifiable elements (e.g., author, creator, time of creation, location) but in other ways defies easy description (the meaning behind the presentation or the context of the photograph).[32] While the retail sector was one of the first to capitalize on using structured and unstructured data, our adversaries are not likely to be far behind. Much as a retailer can combine useful data sets to create a predictive picture of a shopper's behavior, a foreign adversary can create a map of the Air Force with granularity at the individual level or, perhaps more valuably, discern patterns indicative of actions impending or underway by the Air Force or communities within the Air Force.

Adversary Data Theft

To create a useful and predictive picture of the Air Force, an adversary would first need to collect a substantial amount of structured and unstructured data. While it may be attractive to secure this data to keep it out of an adversary's reach, the reality is that much of the data an adversary would need is already easily available. Some is openly shared through unsecured social media posts, but much is obtained through theft, data spillages, and hacks. Two separate hacks of the Office of Personnel Management (OPM) compromised the personal information (including full names, birthdates, financial data, and more) of over 50 million current and former government employees, prospective employees, and family members.[33] While the breach affected many government agencies, all Air Force security clearance holders were in this group. Besides personal information, the hackers also stole biometrics information with a reported 5.6 million sets of fingerprints and the passwords applicants created for the online application process.[34] The theft of passwords is disconcerting given that researchers have found approximately 52 percent of individuals reuse passwords across multiple systems.[35] Other devastating hacks of structured data in 2015 were the theft of 80 million Americans' health insurance information from the nation's second largest health insurer, Anthem Insurance, and a hack of 11 million records from Premera Blue Cross insurance, including billing and biographical data and "clinical records and medical histories."[36] In 2015, the credit monitoring bureau Equifax reported that the financial information of 145 million Americans was stolen.[37] Open source reporting has attributed all these hacks to the Chinese government.[38] While there is likely some overlap in victims, these hacks—all discovered in one 24-month period—represent the theft of personal information of over one-third of the US adult population and include most members of the Air Force. While this data was stolen, much of the data an adversary needs is freely given by Airmen through intentional and unintentional sharing.

Data Freely Given

Data is also freely given; many applications exist explicitly for the purpose of data sharing. Take, for example, the Strava running application that allows users to track and share their running routes. Researchers demonstrated that the accessible user data could be used to identify the physical locations of sensitive military bases overseas, the layout of bases, or individuals such as employees of US intelligence agencies, Navy submariners, Airmen deployed to fight the Islamic State, and even Russian soldiers in Crimea.[39] Other examples of freely shared data from commonly used applications include the group dating app 3fun, which inadvertently revealed data from 1.5 million users, and the women's health app Flo, which exposed intimate health data entered and collected by users.[40] Researchers found that Untappd—an app designed for users to record, rate, and share the beers they drink—identified the travel patterns of Air Force pilots, a senior intelligence officer, and Air Force and Department of Defense (DOD) senior officials.[41] LinkedIn, a prominent online resume repository heavily used by Air Force members, contains the resume information of "740 million members in more than 200 countries and territories worldwide."[42] It is widely reported that foreign intelligence agencies of nation-states such as China use LinkedIn to target US government employees.[43] With so much data already in the hands of our adversaries, the Air Force must proceed with the expectation that data protection alone is insufficient to meet the challenge and should consider the ways this data, stolen or freely given, can be used against us.

Threat

By conducting persistent surveillance, an adversary can detect the movement of forces, preparations for a deployment or combat action, and heightened alert status and discern real-world from deception operations. Collected data can then be stored, enabling retrospective surveillance that can identify not just where an individual is but where they have been, potentially unmasking operations or sensitive locations.[44] Security researchers have found that anonymous data collection is only anonymous prior to scrutiny, and by applying demographic attributes to datasets that had previously been deidentified (the process of anonymizing data prior to sharing), they could unmask individual users with near perfect accuracy.[45] Two key threats the Air Force must consider are how an adversary could create a surveillance framework of a particular Air Force demographic for the purposes of garnering advanced warning of US activities and how that surveillance framework could be used on the battlefield for reconnaissance without requiring physical risk. Together, these threats give an adversary the ability to engage in realtime and retrospective surveillance cheaply and with limited risk, degrading our competitive advantage.

Surveilling the Force for Strategic Warning

Surveilling a population from afar has a long history, and clever adversaries have shown that observable patterns in plain view can be used to identify and exploit information meant to be hidden. Beginning in the early 1960s, the

Soviet Committee for State Security—more commonly known in the West by the Russian abbreviation KGB—began to meticulously catalogue common factors of CIA officers operating abroad under diplomatic cover.[46] To do so, the KBG focused on the bureaucracy inherent to the US government to develop an analytic model consisting of twenty-six indicators to discern the secret from the observable.[47] The KGB's model relied on metadata, focusing on elements of bureaucratic organization that would be consistent regardless of geographic location (for example, item #17, "Positions vacated by agency officers were usually filled by the same.").[48] By focusing on features of US bureaucracy, the KGB was able to discern something hidden through observable patterns. The KGB's model was devastatingly effective and demonstrated the value of metadata in the pre-internet era.[49] With vastly more data available to our adversaries today and access to enormous quantities of cheap, commercially available computing power, a similar model could be developed for Air Force personnel.

Imagine an adversary creating a modern version of the KGB's model wherein individuals are identified based on common features and geographic location, social media posts, or even simple open affiliation with the Air Force. Once an individual was identified, an adversary could monitor their activity and over time identify patterns that could provide early warning of changes, such as preparation for deployment. Algorithms can automate this process by searching for persons of interest, and once identified, indexing them for continued monitoring. Once one Airman is identified, AI can use predictive inferences to find chains of other Airmen linked through similar demographic characteristics.[50] Computing capacity is sufficient that there is no need for an adversary to be discerning in their selection; every Airman once identified could be added to the database. Even if the military member avoids the connected world, their spouses or children likely do not, creating other links for connection. In a pre-internet age, the KGB demonstrated the limits of secrecy by showing that every official secret has an attendant web of people and places, of economy and industry that, once identified, becomes observable.[51] In the 1960s, the CIA suffered because they assumed their system was well protected, failing to see the ways their bureaucracy was "enslaved by habit" and vulnerable to observation: the Air Force must take care not to suffer the same fate.[52]

Reconnaissance without Risk in an Agile Combat Employment Fight

Surveilling the Air Force from afar can provide our adversaries more than just warning of US military activity in advance of conflict. Surveillance can disrupt US war plans, removing the Air Force's ability to maintain the element of surprise. In every US conflict, from the Korean War to today, the Air Force has had the ability to base its aircraft over the horizon, effectively outside of the conflict zone. Enshrined in Air Force doctrine, this strategy is still considered the preferred way of projecting airpower in conflict.[53] Investments by Russia and China in ballistic missiles, long-range cruise missiles, and integrated air defenses have drastically reduced the likelihood that traditional main operating bases will survive initial hostilities; it is likely that in the event of war with either Russia or China, the conflict will begin with the US military on the defensive.[54] In response, the Air Force has developed the operational concept known as Agile Combat Employment (ACE).

In combat application, ACE consists of proactive and reactive maneuver and is designed to counter Russia's and China's efforts to defeat our traditional war-fighting strengths.[55] Consequently, survivability through movement is a defining feature of ACE.[56] In place of the safe haven model, ACE envisions rapid independent maneuver of Air Force elements to dispersed operating locations.[57] By identifying the right target population and conducting this surveillance persistently and from afar, our adversaries have the potential to identify dispersal sites prior to our force's arrival or even to intercept our force while traveling between locations, significantly reducing the lifespan of a dispersal location or even precluding its use.

An open-source investigation of Malaysia Airlines Flight 17 is illustrative of the point. On July 17, 2014, the commercial airliner was shot down by a Russian BUK missile while flying above eastern Ukraine en route to Kuala Lumpur.[58] Rather than admit to having provided BUK missiles to separatist forces, Russia and their proxy forces fighting in Ukraine gave a series of increasingly unlikely explanations of what happened while denying the presence of Russian BUK missile systems in Ukraine.[59] However, open-source researchers used Twitter, Facebook, and other local social media platforms along with leaked cellphone location data and Google Earth imagery to construct a timeline of the BUK's arrival in Ukraine from Russia.[60] They identified the route of the missile, the individuals involved in the operation, and photographs of the vehicle convoy as it made its way through Ukraine.[61]

If the US were to go to war with Russia, the Russian government could use the same technology to pinpoint the location of US forces and their intended destination. By following the Airmen's social media and cellular data along with the social media buzz of unaffiliated civilians reporting on the movement of Airmen, the Russians could effectively monitor US forces without using anything more sophisticated than openly available data coupled with AI to analyze the data rapidly. If the Russians wished, they could enhance this passive collection with more invasive and provocative forms of data collection, such as identifying and tracking the comings and goings of military personnel outside of US installations and using license plate readers (LPR) or international mobile subscriber identity (IMSI) catchers (the IMSI is a mobile phone's unique serial number; IMSI catchers record which cellphones are present in a specific location). Combining data collection from afar with strategies such as adding LPRs or IMSI catchers would effectively create a fence around an overseas installation, allowing an adversary to observe real-time movement of US forces from the installation. While it would be a provocative step to place physical surveillance devices outside of our installations overseas, foreign adversaries have already done so in the United States, with IMSI catchers found in the Washington, DC, area in 2017 in close proximity to sensitive locations including the White House.[62] The prevalence of this technology, the low cost and small size of the devices, and lack of physical infrastructure needed to support them would present a cost-effective risk versus reward opportunity to an adversary. The US can take steps to look for physical devices such as IMSI catchers or LPRs, but if these devices are difficult to find inside the US, the challenge is certainly greater in a foreign environment where US counterintelligence capabilities are constrained by the host nation. Critically, while LPRs or IMSI catchers may enhance the abilities of our adversaries, they are by no means necessary to conduct surveillance and reconnaissance of US forces using the openly observable data we produce.

Success in an ACE fight requires moving our forces from locations known to our adversary to destinations unknown to our adversary. Adversaries surveilling our force using data derived from the combination of social media, IoT sensors, and other data-producing activities can watch the movement of our forces in real time. AI can take the observation a step further by offering predictive insights into the likely destination of those forces. The effect of these actions is to allow adversaries to conduct reconnaissance without risk to their forces. Other technical means such as satellites also allow for reconnaissance without risk, but a satellite does not offer the insight of the human dimension, the living thoughts of the Airmen on the move. The human dimension enhances prediction and provides a powerful potential tool to disrupt the maneuver of our forces.

Safeguards and Mitigation

There are two distinct but related facets to the vulnerability derived from ubiquitous data creation. The first facet this paper has focused on is the vulnerability of the Air Force to exploitation through the mass surveillance of individual Airmen. The second facet implicit in this vulnerability is the personal risk to the Airman as an individual, outside the risk to any Air Force operation. To address the first aspect of the vulnerability, the Air Force should focus on the second. If the Air Force's greatest OPSEC threat is the ubiquitous nature of data collection permeating every aspect of an Airman's life, then remedies limited to the professional sphere will be insufficient to solve the problem. The Air Force must create a culture of digital awareness that extends into Airmen's private lives.

There is a tricky balance to navigate in this regard; Airmen have a right to a private life. Because much of the way we interact with the connected world is through personal expression, there is a valid concern that government efforts to influence online activities will amount to violations of First Amendment freedoms or government censorship. It is neither reasonable nor expected that Airmen forgo all use of social media or connected devices. Even if that were the case, it would be unlikely to meaningfully limit data collection because of the abundance of sensors collecting data that are hardwired into the environment. Maintaining total anonymity is beyond the reach of most individuals.[63] However, the threat can be reduced by educating Airmen on how their interaction with the internet can affect themselves and the Air Force mission and the precluding actions they can take. The goal is to influence the choices Airmen make and in turn mitigate the vulnerability.

A Framework of Harm

The Air Force can influence but not control an individual's personal online habits. The degree of influence it will have over Airmen's online habits is likely to correlate to the relevance and importance they subjectively place on the potential harm their lack of compliance will cause. When educating the force on the risks posed by the digital environment, the Air Force should emphasize the distinction between what behavior economists describe as subjective and objective privacy harms.[64]

A subjective privacy harm is essentially unwanted spying; the individual's data is being captured and exploited in a way that makes them uncomfortable. Subjective harms take many forms but include "the psychological discomfort associated with feeling surveilled or the embarrassment associated with public exposure of sensitive information."[65] By contrast, objective harms can be "immediate and tangible, or indirect and intangible" and include a range of harms from identity theft to being targeted by terrorists and the possibility your information is feeding a foreign adversary's surveillance and reconnaissance efforts.[66]

For most Airmen, their greatest personal risk is subjective harm. Airmen have proven vulnerable to sextortion schemes, fraud schemes, online harassment, and other challenges that can be mitigated by education and modifying online practices. If appropriately educated, Airmen can understand the ways these subjective harms can objectively endanger the Air Force mission.

Airmen who take steps to reduce their online vulnerabilities are simultaneously reducing the Air Force's vulnerability. Appeals to limit or modify online behavior based on the potential of an adversary weaponizing the individual's online activity is unlikely to resonate with many, especially junior Airmen. They may view the outcome of their individual activity as intangible and unlikely to affect the Air Force as a whole.

The Air Force makes a concerted effort to educate Airmen on life skills not directly connected to their specific Air Force specialty. For example, Air Force Instruction 1-1, *Air Force Standards*, highlights numerous areas where aspects of personal life intersect with the professional, such as appearance, fitness, financial responsibility, and dependent care responsibilities.[67] Education programs on these life skills are presented as a subjective benefit to the individual but also benefit the Air Force by improving the readiness of its members. Educating Airmen to be more privacy-conscious online—to understand what data they are creating and how it can be used—benefits the Air Force mission and the individual Airman.

Current Policy and Training

For the average Airman, OPSEC training consists primarily of DOD-mandated online training.[68] The training includes discussion of personal vulnerabilities, particularly online, but not the tools an Airman would need to implement any personal safeguards.[69] OPSEC policy is almost exclusively focused on the impact to the military mission. AFI 10-701, *Operations Security*, refers to social media exactly once—and only in the context of prohibiting posting sensitive details to social media without appropriate oversight (no distinction is made between official and unofficial social media platforms).[70] No mention is made of the vulnerability of geolocation, publicly accessible metadata, or other tools an adversary could use to glean useful data on Air Force operations and members.

To the extent commanders are charged with evaluating their unit's OPSEC profile, it is within the context of an operational activity.[71] The Air Force is not unaware of the gap between current education tools and the vulnerability of Airmen online. In January 2021, elements from the Air Staff conducted a staff study seeking to identify ways to "protect Airmen against online fraud, impersonation, mis/disinformation and cybercrime activities."[72] While an important acknowledgement of a gap in awareness, the study aimed primarily to address potential subjective harm to Airmen and did not address the objective harm of mass surveillance of the Air Force. The DOD has also taken initial steps to combat the threat posed by connected devices and data collection, focusing primarily on deployed forces. After the vulnerabilities exposed by the Strava running app came to light, Deputy Secretary of Defense Patrick Shanahan issued a memorandum. It acknowledged the risk posed by geolocation data sharing and prohibited the use of geolocation features in either government or personal devices within a designated operational area.[73]

The Air Force considers OPSEC to be everyone's responsibility but requires commanders to develop and implement OPSEC programs for their organizations.[74] OPSEC programs as currently conceived focus on protecting the unit's critical information. What constitutes critical information requires a level of knowledge of enemy capabilities and intentions that most commanders lack.[75] Air Force OPSEC policy orients a commander's attention to the activities of their unit in the context of the work environment, particularly "identifying and managing signatures associated with Air Force activities, capabilities, operations, and programs."[76] This focus neglects the ubiquitous nature of data collection that flows through Airmen and their families. Further, the Air Force does not give commanders the education or policy foundation to understand or mitigate the threat to their unit posed by their Airmen's online activity. For any change to make a meaningful impact, it must occur servicewide and not vary based on a commander's abilities, interests, or personal background knowledge of the subject.

Recommendation: Education as a Countermeasure

Air Force policy takes a countermeasures-oriented approach to addressing OPSEC vulnerabilities.[77] Because people are the source of the vulnerability, a key countermeasure begins with educating Airmen and their families. The Air Force should integrate training on the vulnerabilities inherent to social media, geolocation data, and metadata collection beginning at initial entry and continuing throughout the Airman's career. Using a framework of educated awareness, all Airmen should be informed appropriate to their mission and relative position in an organization. Educated awareness is an overarching approach where knowledge and understanding rather than a single prescriptive solution or policy deepen the resiliency of the force.[78]

By ensuring Airmen understand how they are vulnerable to exploitation, they will be more likely to take steps to mitigate or minimize their risk. Training should be focused on the intersection of the internet and the Airman and include real-world examples of how data can be used against Airmen to address the common risks they will encounter. For instance, first-term Airmen have been proven particularly vulnerable to online sextortion scams.[79] Through a concerted, sustained education campaign, Airmen will benefit in their personal and professional lives.

By educating the force beginning with accession and continuing throughout their military service, Airmen can be empowered to make smart choices that will enhance their personal readiness. They will also have a framework for understanding how their information can be exploited and operationalized against the Air Force through multiple phases of conflict. Much like the Air Force seeks to create a culture where fitness habits are ingrained and reinforced through positive feedback, an Airman's online habits can be shaped through education and reinforcement—benefiting the service and the servicemember. Focusing on the individual Airman is important, but changing the culture across the Air Force necessarily includes more than education at the individual level. To meet the challenge, the Air Force must bring together disparate communities to address the larger bureaucracy where OPSEC policy and culture reside.

Recommendation: A Team Approach

A key challenge to addressing the threat posed by the ubiquitous nature of data collection is the lack of a single operational stakeholder; education, policy, and operations fall across multiple functional communities. History has shown bureaucratic inertia can inhibit the US government's learning process, especially when problems or solutions fall "between barstools."[80] When a problem is distributed across a wide range of players, implementing change becomes the simultaneous responsibility of everyone and no one—dramatically reducing the likelihood of identifying or implementing needed changes.[81] The Air Force should consider this problem as a multidisciplinary challenge and leverage a wide range of practitioners to develop servicewide solutions. While planning teams incorporate OPSEC into wargaming, Airmen in all specialties should incorporate OPSEC into their training even though it may not seem directly related to their military specialty.

Recommendation: Realistic Training to Foster Creative Solutions

Because the Air Force conceives of its operational environment in the third dimension, there is a potential to fail to adequately address vulnerabilities on the ground. With few exceptions, most Airmen receive only rudimentary training in ground combat operations. The Air Force should incorporate realistic training on the threats posed by the IoT and social media into the full range of training activities, from deployment preparation to installation-level training. The goal is to sensitize the force to the threat and prepare Airmen to develop creative solutions in communication constrained environments. There may be a role for a technology-based solution wherein the Air Force invests in systems or capabilities to counter metadata-driven surveillance, but all Airmen would benefit from tactical-level awareness of the challenge. If Airmen are sufficiently aware of the threat posed by social media, cellphones, smart watches, their vehicle's embedded GPS, and other exploitable features of the modern environment, they will have a base of knowledge enabling them to develop smart countermeasures at the local level to deal with these challenges. The goal is not total disengagement from the connected world we occupy. However, by engaging in a continuous cycle of training and education of the vulnerabilities associated with modern technologies, Airmen will be better positioned to mitigate current and future vulnerabilities.

Conclusion

US adversaries can track the Air Force as a population using a mixture of freely given and stolen data. Doing so is in line with long-standing intelligence practices to surveil your adversaries for the purpose of strategic warning and the conduct of reconnaissance during or immediately prior to hostilities. While commercial entities closely surveil their target demographic for the purpose of generating business, foreign adversaries are likely capitalizing on the opportunity to similarly surveil US forces. Additionally, the increasing ability to harness emerging technologies such as AI and machine learning to analyze and predict events will allow adversaries to surveil with greater accuracy and automation. The risk posed by this threat can be reduced through straightforward actions. A key component to understanding risk is realizing the harm to or impact on achievement of the objective if the risk remains unaddressed.[82]

While assessing risk is difficult when lacking historical examples for comparison, the implications are clear. In response to these challenges, recent Army and Marine deployments have experimented with prohibiting personnel from bringing any personal electronic devices with them.[83] Reducing the number of such devices each servicemember possesses on a deployment is useful, but it does not address the risk to forces in garrison worldwide. The Air Force is particularly vulnerable in this area considering the over-the-horizon aspect of Air Force basing. For the Air Force, the distinction between being in garrison and deployed is less meaningful than for other services. If the Air Force is to remain at a competitive advantage, its members must understand the threat the digital environment poses. The Air Force approach to this threat is built on the foundation of an OPSEC program that does not address today's sensing and computing environment.

Air Force tactics center on operations in the third dimension and, increasingly, the cyber realm. This orientation affects how the Air Force prepares its forces for war. The average Airman is not exposed to hostile fires and historically has benefited from operating from an installation defended from ground and air attack. Knowing the locations of our Air Force bases is of little value to an enemy unable to strike them. However, this advantage will not hold in the event of a conflict with our near-peer adversaries who are more likely to exploit an OPSEC vulnerability.[84] The future vision for the Air Force is forces maneuvering quickly, in small teams, and operating from locations vulnerable to ground and air attack. Garrisoned forces in the United States are within the digital reach of our adversaries. Surveillance is now possible at scale, which requires rethinking how Airmen interact with technology professionally and in their personal lives. Because adapting to this threat will not be the purview of any single specialty, successful change will require overcoming bureaucratic preferences to "adapt only slowly and incrementally."[85] Bringing the Air Force's operations security culture into the twenty-first century will benefit Airmen personally and reduce vulnerability in Air Force operations. Failure to take this action gives our adversaries an opportunity to degrade the Air Force's success on a future battlefield. The Air Force knows it must change or risk losing its dominance.[86] While the Air Force is focused on reinvigorating its war-fighting approach, it has so far neglected to address a key vulnerability that will undermine future Air Force operations. To ensure future dominance, the Air Force must recognize the vulnerability posed by population-level surveillance and adopt a twenty-first-century approach to operations security.

Notes

(All notes appear in shortened form. For full details, see the appropriate entry in the bibliography.)

1. US Department of State, Bureau of Consular Affairs, "China International Travel: Local Laws and Special Circumstances."

2. Air Force Instruction (AFI) 10-701, *Operations Security (OPSEC)*, para. 1.3.

3. Gentry and Gordon, *Strategic Warning Intelligence*, 152.

4. Senate, *Open Hearing: Nomination of Ambassador William Burns to be Director of the Central Intelligence Agency: Additional Prehearing Questions for William J. Burns*, 117th Cong., 1st sess. (2021), 5.

5. Gentry and Gordon, *Strategic Warning Intelligence*, 152.

6. Gentry and Gordon, 152.

7. Tucker, *Naked Future*, 6.

8. Marr, *Big Data*, 10.

9. Feldstein, "Global Expansion of AI Surveillance," 5.

10. Voice of America, "Words and Their Stories: Loose Lips Sink Ships."

11. Association of National Advertisers (ANA) Educational Foundation, "Security of War Information – Loose Lips Sink Ships (1942–1945)."

12. Johnson, *Thwarting Enemies at Home and Abroad*, 1.

13. Feldstein, "Global Expansion of AI Surveillance," 2.

14. Tucker, *Naked Future*, 120.

15. Buchanan, *Hacker and the State*, 235.

16. Headquarters Air Force (HAF)/A3CX, memorandum, subject: Digital Force Protection Team Findings, 1.

17. Schneier, *Data and Goliath*, 23; and Buchanan, *Hacker and the State*, 38.

18. Schneier, 23.

19. Singer and Brooking, *LikeWar*, 111–14.

20. Curtis E. LeMay Center for Doctrine Development and Education, "Air Force Doctrine Publication 3-13, Information Operations."

21. Singer and Brooking, *LikeWar*, 46–49.

22. Tunnicliffe and Tatham, *Social Media*, 2.

23. Marr, *Big Data*, 58.

24. Schneier, *Data and Goliath*, 35.

25. Tucker, *Naked Future*, 8.

26. Tucker, 11; and Gavin, "How Big Are Gigabytes?"

27. Gavin, 11.

28. Gavin, 60.

29. Gavin, 60.

30. Gavin, 60.

31. Gavin, 61.

32. Gavin, 61.

33. Office of Personnel Management (OPM), "Cybersecurity Resource Center."

34. OPM, "Cybersecurity Resource Center."

35. Wang et al., "Next Domino to Fall," 196–203.

36. Buchanan, *Hacker and the State*, 107.

37. Buchanan, 107.

38. Buchanan, 107.

39. Hern, "Fitness Tracking App Strava"; and Postma, "After Strava."

40. Porter, "Group Dating App"; and Gupta and Singer, "Your App Knows You Got Your Period."

41. Postma, "Military and Intelligence Personnel Can Be Tracked."

42. LinkedIn, "About."

43. Lucas, "People Are Looking at Your LinkedIn Profile."

44. Schneier, *Data and Goliath*, 34.

45. Rocher and de Montjoye, "Estimating the Success of Re-identifications."

46. Haslam, "Near and Distant Neighbors," 253.

47. Haslam, 255.

48. Haslam, 257.

49. Haslam, 257.

50. Schneier, *Data and Goliath*, 38.

51. Paglen, *Blank Spots on the Map*, 17.

52. Haslam, "Near and Distant Neighbors," 255.

53. Curtis E. LeMay Center for Doctrine Development and Education, "How We Do It: Tenets of Airpower," 11–15.

54. Vick, *Air Base Attacks*, 35.

55. Brown, *Agile Combat Employment (ACE): PACAF Annex*, 2. See also Curtis E. LeMay Center for Doctrine Development and Education, "Air Force Doctrine Note 1-21, Agile Combat Employment."

56. Reilly, "Agile Combat Employment (ACE) Concept of Operations," slide 12.

57. Reilly, slide 15.

58. BBC News, "MH17 Ukraine Plane Crash."

59. Associated Press, "Latest: Putin Denies Russia Responsible."

60. Bellingcat, "MH17: The Open Source Investigation."

61. Toler, "MH17 in Their Own Words."

62. Timburg, "Signs of Sophisticated Cellphone Spying."

63. Schneier, *Data and Goliath*, 43.

64. Acquisti, "Economics and Behavioral Economics of Privacy," 83.

65. Acquisti, 83.

66. Acquisti, 83.

67. AFI 1-1, *Air Force Standards*.

68. HAF/A3CX, memorandum, subject: Digital Force Protection Team Findings, para. 5(a)(1).

69. Department of the Air Force. "Operations Security Awareness Training, 2022."

70. AFI 10-701, *Operations Security*, para. 1.8.4.

71. AFI 10-701, para. 3.7.

72. HAF/A3CX, memorandum, subject: Digital Force Protection Team Findings, para. 4(a).

73. Shanahan to Department of Defense senior leaders, memorandum, 8.

74. AFI 10-701, *Operations Security*, para. 1.7.

75. Joint Publication 3-13.3, *Operations Security*, II-3–II-4.

76. AFI 10-701, *Operations Security*, para. 1.6.

77. AFI 10-701, para. 1.10.

78. HAF/A3CX, memorandum, subject: Digital Force Protection Team Findings, para. 6(a).

79. Ng, "Sextortion Scam Hits US Military."

80. Komer, *Bureaucracy Does Its Thing*, ix.

81. Komer, ix.

82. Joint Publication 5-0, *Joint Planning*, xiv.

83. Athey, "Are Phoneless Deployments the Future for Marines?"

84. Paul, *Information Operations Doctrine and Practice*, 79.

85. Komer, *Bureaucracy Does Its Thing*, xii.

86. Brown, "Accelerate Change or Lose," 3.

Abbreviations

ACE	Agile Combat Employment
AI	artificial intelligence
DOD	Department of Defense
IMSI	international mobile subscriber identity
IoT	Internet of Things
LPR	license plate reader
OPM	Office of Personnel Management
OPSEC	operations security

Bibliography

Acquisti, Alessandro. "The Economics and Behavioral Economics of Privacy." In *Privacy, Big Data, and the Public Good: Frameworks for Engagement*, edited by Julia Lane et al., 76–95. New York: Cambridge University Press, 2014.

Air Force Instruction 1-1. *Air Force Standards*, August 7, 2012 (Incorporating Change 1, November 12, 2014).

Air Force Instruction 10-701. *Operations Security (OPSEC)*, July 24, 2019 (Incorporating Change 1, June 9, 2020). https://static.e-publishing.af.mil/.

Association of National Advertisers (ANA) Educational Foundation. "Security of War Information – Loose Lips Sink Ships (1942–1945)." Accessed July 2022. https://aef.com/.

Athey, Phillip. "Are Phoneless Deployments the Future for Marines?" *Defense News*, November 16, 2020. https://www.defensenews.com/.

BBC News. "MH17 Ukraine Plane Crash: What We Know," February 26, 2020. https://www.bbc.com/.

Bellingcat. "MH17: The Open Source Investigation Three Years Later," 2017. https://www.bellingcat.com/.

Brown, Gen Charles Q. "Accelerate Change or Lose." Office of the Chief of Staff, US Air Force, August 2020. https://www.af.mil/.

———. *Agile Combat Employment (ACE): PACAF Annex to Department of the Air Force Adaptive Operations in Contested Environments*. Honolulu, HI: Headquarters Pacific Air Forces, June 2020.

Buchanan, Ben. *The Hacker and the State: Cyber Attacks and the New Normal of Geopolitics*. Cambridge, MA: Harvard University Press, 2020.

Curtis E. LeMay Center for Doctrine Development and Education. "Air Force Doctrine Note 1-21, Agile Combat Employment," December 1, 2021. https://www.doctrine.af.mil/Portals/.

———. "Air Force Doctrine Publication 3-13, Information Operations," April 28, 2016. https://www.doctrine.af.mil/Portals/61/documents/Annex_3-13/3-13-D01-INFOIntroduction.pdf.

———. "How We Do It: Tenets of Airpower." In Air Force Doctrine Publication 1, *The Air Force*, 11–15, March 10, 2021. https://www.doctrine.af.mil/.

Department of Defense Directive 1344.10. *Political Activities by Members of the Armed Forces*, February 19, 2008.

Department of the Air Force. "Operations Security Awareness Training, 2022." Required annual training accessed through My Learning.

Feldstein, Steven. "The Global Expansion of AI Surveillance." Working Paper. Washington, DC: Carnegie Endowment for International Peace, September 2019. https://carnegieendowment.org/.

Gavin, Brady. “How Big Are Gigabytes, Terabytes, and Petabytes?” How-To Geek, May 25, 2018. https://www.howtogeek.com/.

Gentry, John A., and Joseph S. Gordon. *Strategic Warning Intelligence: History, Challenges, and Prospects*. Washington, DC: Georgetown University Press, 2019.

Gupta, Alisha Haridasani, and Natasha Singer. “Your App Knows You Got Your Period. Guess Who It Told?” *New York Times*, January 28, 2021. https://www.nytimes.com/.

Haslam, Jonathan. *Near and Distant Neighbors: A New History of Soviet Intelligence*. New York: Farrar, Strauss, and Giroux, 2015.

Headquarters Air Force (HAF)/A3CX. Memorandum. Subject: Digital Force Protection Team Findings, January 2021.

Hern, Alex. “Fitness Tracking App Strava Gives Away Location of Secret US Army Bases.” *Guardian*, January 28, 2018. https://www.theguardian.com/.

House. 2016 National Defense Authorization Act. Public L. No. 114-92. 114th Cong.

Johnson, William R. *Thwarting Enemies at Home and Abroad: How to Be a Counterintelligence Officer*. Washington, DC: Georgetown University Press, 2009.

Joint Publication 3-13.3. *Operations Security,* January 6, 2016. https://media.defense.gov/.

Joint Publication 5-0. *Joint Planning*, December 1, 2020. https://www.jcs.mil/.

Komer, Robert W. *Bureaucracy Does Its Thing: Institutional Constraints on USGVN Performance in Vietnam*. Santa Monica, CA: RAND Corporation, 1972. https://www.rand.org/.

LinkedIn. “About LinkedIn.” Accessed March 8, 2021. https://about.linkedin.com/.

Lucas, Ryan. “People Are Looking at Your LinkedIn Profile. They Might Be Chinese Spies.” National Public Radio, September 19, 2019. https://www.npr.org/

Marr, Bernard. *Big Data: Using Smart Big Data Analytics and Metrics to Make Better Decisions and Improve Performance*. Chichester, UK: Wiley, 2015.

Ng, Alfred. “Sextortion Scam Hits US Military below the Belt.” CNET, November 29, 2018. https://www.cnet.com/.

Office of Personnel Management. “Cybersecurity Resource Center: Cybersecurity Incidents.” Accessed March 8, 2021. https://www.opm.gov/.

Paglen, Trevor. *Blank Spots on the Map: The Dark Geography of the Pentagon’s Secret World*. New York: Dutton, 2009.

Paul, Christopher. *Information Operations Doctrine and Practice: A Reference Handbook*. Westport, CT: Praeger Security International, 2008.

Porter, Jon. “Group Dating App Found Leaking Basically Everything about Its Users Worldwide: All of Its 1.5M Users Had Their Data Exposed.” The Verge, August 9, 2019. https://www.theverge.com/.

Postma, Foeke. “After Strava, Polar Is Revealing the Homes of Soldiers and Spies.” Bellingcat, July 8, 2018. https://www.bellingcat.com/.

———. “Military and Intelligence Personnel Can Be Tracked with the Untappd Beer App.” Bellingcat, May 18, 2020. https://www.bellingcat.com/.

Reilly, Jeffrey M. “Agile Combat Employment (ACE) Concept of Operations.” Air University, November 21, 2019.

Rocher, Luc, Hendrickx, J. M., and de Montjoye, Y. A. “Estimating the Success of Re-Identifications in Incomplete Datasets Using Generative Models.” *Nature Communications* 10, no. 3069: 2019. https://doi.org/10.1038/s41467-019-10933-3.

Schneier, Bruce. *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World*. New York: W. W. Norton & Company, 2015.

Senate. *Open Hearing: Nomination of Ambassador William Burns to be Director of the Central Intelligence Agency: Additional Prehearing Questions for William J. Burns*. 117th Cong., 1st sess. (2021). https://www.intelligence.senate.gov/.

Shanahan, Patrick M., Deputy Secretary of Defense, Department of Defense. To Department of Defense senior leaders. Memorandum. Subject: Use of Geolocation-Capable Devices, Applications and Services, August 3, 2018.

Singer, P. W., and Emerson T. Brooking. *LikeWar: The Weaponization of Social Media*. New York: Houghton Mifflin, 2018.

Tucker, Patrick. *The Naked Future: What Happens in a World That Anticipates Your Every Move?* New York: Penguin Group, 2014.

Tunnicliffe, Ian, and Steve Tatham. *Social Media—The Vital Ground: Can We Hold It?* The Letort Papers. Carlisle, PA: Strategic Studies Institute and US Army War College Press, 2017.

US Department of State, Bureau of Consular Affairs. “China International Travel: Local Laws and Special Circumstances.” Accessed July 2022. https://travel.state.gov/.

Vick, Alan J. *Air Base Attacks and Defensive Counters: Historical Lessons and Future Challenges*. Santa Monica, CA: RAND Corporation, 2015. https://www.rand.org/.

Voice of America. “Words and Their Stories: Loose Lips Sink Ships,” October 2019. https://learningenglish.voanews.com/.

Wang, Chun, Steve T. K. Jan, Hang Hu, Douglas Bossart, and Gang Wang. “The Next Domino To Fall: Empirical Analysis of User Passwords across Online Services,” 196–203. In *Proceedings of the Eighth ACM Conference* *on Data and Applications Security and Privacy (CODASPY)* (Tempe, AZ, March 2018). New York: Association for Computing Machinery, 2018. https://doi.org/10.1145/3176258.3176332.

AIR UNIVERSITY PRESS

https://www.airuniversity.af.edu/AUPress/

ISSN 2687-7260