
# NAVAL POSTGRADUATE SCHOOL

**MONTEREY, CALIFORNIA**

# THESIS

**CAN YOU HEAR ME NOW?**
**THE VULNERABILITY OF CELLULAR AND SMARTPHONE USE ON THE BATTLEFIELD**

by

Erich Eshelman

June 2020

Thesis Advisor: Ryan Maness
Second Reader: Kristen Tsolis

**Approved for public release. Distribution is unlimited.**

THIS PAGE INTENTIONALLY LEFT BLANK

| REPORT DOCUMENTATION PAGE | *Form Approved OMB No. 0704-0188* |
|---|---|



| **1. AGENCY USE ONLY** *(Leave blank)* | **2. REPORT DATE** June 2020 | **3. REPORT TYPE AND DATES COVERED** Master's thesis |
|---|---|---|

**4. TITLE AND SUBTITLE**
CAN YOU HEAR ME NOW? THE VULNERABILITY OF CELLULAR AND SMARTPHONE USE ON THE BATTLEFIELD

**5. FUNDING NUMBERS**

**6. AUTHOR(S)** Erich Eshelman

**7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)**
Naval Postgraduate School
Monterey, CA 93943-5000

**8. PERFORMING ORGANIZATION REPORT NUMBER**

**9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)**
N/A

**10. SPONSORING / MONITORING AGENCY REPORT NUMBER**

**11. SUPPLEMENTARY NOTES** The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

**12a. DISTRIBUTION / AVAILABILITY STATEMENT**
Approved for public release. Distribution is unlimited.

**12b. DISTRIBUTION CODE**
A

**13. ABSTRACT (maximum 200 words)**

Enemies of the United States of America seek new asymmetric means to counter the strength of the American military. The rise in the use of cellular and smartphones around the globe has created new threats for military forces. This thesis shows cellular and smartphones are a medium for dissemination of propaganda and cyberspace exploitation, and thus are a focus for operational security concerns. The 2014 Russian invasion of Crimea and the subsequent occupation of Eastern Ukraine presents an excellent case study to examine the vulnerabilities of these devices. The war in Ukraine shows the use of text messages to spread propaganda, the manipulation of a Ukrainian fire support Android application to give away the location of its user to the enemy, and the dangers of OPSEC violations through social media posts to give away important military information. This thesis also examined the future threats to these vulnerable devices and their possible effects on the United States. The rise of 5G technology, deepfake videos, and vulnerabilities in the IoT all offer new vectors to attack and exploit American service members. Prescriptive measures the United States can employ through effective training and education are presented to ensure service members know the reason why their phones cannot be used. The thesis suggests this training needs to be applied to the allies and partner forces of the United States as well, to ensure their survival on the modern battlefield.

| **14. SUBJECT TERMS** | **15. NUMBER OF PAGES** |
|---|---|
| Ukraine, IO, cellular phones, mobile phones, smartphones, Russia, vulnerabilities, exploitation, EW, cyberspace exploitation, Operational Security, OPSEC, propaganda, open source intelligence, OSINT, IW, information warfare, information operations, social media | 109 |
| | **16. PRICE CODE** |

| **17. SECURITY CLASSIFICATION OF REPORT** | **18. SECURITY CLASSIFICATION OF THIS PAGE** | **19. SECURITY CLASSIFICATION OF ABSTRACT** | **20. LIMITATION OF ABSTRACT** |
|---|---|---|---|
| Unclassified | Unclassified | Unclassified | UU |

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

**Approved for public release. Distribution is unlimited.**

**CAN YOU HEAR ME NOW? THE VULNERABILITY OF CELLULAR AND SMARTPHONE USE ON THE BATTLEFIELD**

Erich Eshelman
Major, United States Army
BS, U.S. Military Academy, 2007

Submitted in partial fulfillment of the
requirements for the degree of

**MASTER OF SCIENCE IN INFORMATION STRATEGY AND POLITICAL WARFARE**

from the

**NAVAL POSTGRADUATE SCHOOL**
**June 2020**

Approved by: Ryan Maness
Advisor

Kristen Tsolis
Second Reader

Kalev I. Sepp
Chair, Department of Defense Analysis

THIS PAGE INTENTIONALLY LEFT BLANK

# ABSTRACT

Enemies of the United States of America seek new asymmetric means to counter the strength of the American military. The rise in the use of cellular and smartphones around the globe has created new threats for military forces. This thesis shows cellular and smartphones are a medium for dissemination of propaganda and cyberspace exploitation, and thus are a focus for operational security concerns. The 2014 Russian invasion of Crimea and the subsequent occupation of Eastern Ukraine presents an excellent case study to examine the vulnerabilities of these devices. The war in Ukraine shows the use of text messages to spread propaganda, the manipulation of a Ukrainian fire support Android application to give away the location of its user to the enemy, and the dangers of OPSEC violations through social media posts to give away important military information. This thesis also examined the future threats to these vulnerable devices and their possible effects on the United States. The rise of 5G technology, deepfake videos, and vulnerabilities in the IoT all offer new vectors to attack and exploit American service members. Prescriptive measures the United States can employ through effective training and education are presented to ensure service members know the reason why their phones cannot be used. The thesis suggests this training needs to be applied to the allies and partner forces of the United States as well, to ensure their survival on the modern battlefield.

THIS PAGE INTENTIONALLY LEFT BLANK

# TABLE OF CONTENTS

# LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

# LIST OF ACRONYMS AND ABBREVIATIONS

| | |
|---|---|
| BS | Base Station |
| BSC | Base Station Controller |
| CDMA | Code Division Multiple Access |
| GPS | Global Positioning System |
| GSM | Global System for Mobile Communications |
| HLR | Home Location Register |
| IA | Information Assurance |
| IDF | Israeli Defense Force |
| IMSI | International Mobile Subscriber Identity |
| IO | Information Operations |
| IoT | Internet of Things |
| ISR | Intelligence Surveillance Reconnaissance |
| IW | Information Warfare |
| MISO | Military Information Support Operations |
| MME | Mobile Management Entry |
| MS | Mobile Station |
| MSC | Mobile Switching Center |
| NATO | North Atlantic Treaty Organization |
| NGW | New Generation Warfare |
| OPFOR | Opposing Force |
| OPM | Office of Personnel Management |
| OPSEC | Operational Security |
| OSINT | Open Source Intelligence |
| PSTN | Public Switched Telephone Network |
| SMS | Short Message Service |
| TMSI | Temporary Mobile Subscriber Identity |
| TORPEDO | Tracking via Paging mEssage DistributiOn |
| UAV | Unmanned Aerial Vehicle |
| VLR | Visitor Location Register |

THIS PAGE INTENTIONALLY LEFT BLANK

# ACKNOWLEDGMENTS

I am indebted to my loving wife for her care to our family and her critical eye to my writing. She has struggled with me through the difficulties of a military career, from the fears during deployment, to the agony of jumpmaster school years ago, to the current boredom of learning a new set of nomenclature as I describe how cellular phones and networks operate. Even when I have brought her to beautiful Monterey, California, there is still difficulty. She endures these hardships with a smile and an unbelievable calm in the face of my rants and our son's tantrums (these are sometimes one and the same). Thank you. I love you!

To my advisors, Professor Ryan Maness and Kristen Tsolis, thank you for the care and energy you spent helping this idea of mine come to fruition. The discussions we had and the resources and contacts you shared were invaluable. Thank you for helping to make this a successful thesis.

To COL Curtis Taylor and LTC Richard Johnson, thank you for taking time from your busy schedules to answer questions and talk about the vulnerabilities of cellular and smartphone use as you see it from your respective units. My hope is that the Security Force Assistance Brigades and the Operations Group at JRTC can benefit from this research.

MSG Rondriques Jackson, thank you for continuing to assist me, even though it has been too many years since we have seen each other in person. You are a phenomenal Non-Commissioned Officer, Battle Buddy, and most importantly, friend. Cobra Strike!

The Graduate Writing Center, and more specifically, Dr. Cheryldee Huddleston, has turned a barely-literate, former "cannon cocker" into a successful graduate student. Dr. Huddleston is a treasure to NPS, and her assistance to students, especially those in the Defense Analysis program, cannot be understated. She has struggled away with me as we navigated the rough waters of my thesis journey and ensured I emerged successful. Thank you!

To my son, James, thank you for the distractions from the constant reading and writing. Sheltering in place during the COVID-19 pandemic has been a lot more fun because of you. Especially with all the Lego models we have built. I love you!

In loving memory of our daughter, Eliza Eshelman. You never saw the beauty of this world, but you also never experienced its dangers. We will love you forever.

# I. INTRODUCTION

Adversaries of the United States have sought to use asymmetric means to disrupt American military efforts. The increasing popularity of cellular and smartphones in the general population has brought a new threat to this asymmetric environment. This thesis examines three particular risks from smartphones: propaganda, cyberspace exploitation, and operational security (OPSEC) concerns. The Russians, during their 2014 invasion of Ukraine, introduced "pinpoint propaganda" via targeted text messages to the personal cell phones of Ukrainian soldiers. These Russian techniques sought to degrade the morale of the Ukrainian Defense Force and cause desertion. Cyberspace exploitation will focus on the hacking of a Ukrainian Artillery Android Application that enabled the Russians to target Ukrainian artillery batteries. Careless posting on social media will illustrate OPSEC concerns by Russian troops. These OPSEC vulnerabilities will be highlighted in actions that ran counter to President Vladimir Putin's denial of Russian forces in Ukrainian territory and in strong evidence procured by Open Source Intelligence (OSINT) collector Bellingcat that shows Russian forces downed Malaysian Airways Flight 17 over Ukraine. Mobile phones add new threats and vulnerabilities to a long list already faced by military commanders. This thesis seeks to explore the new vulnerabilities cellular phones introduce to the battlefield.

## A. METHODOLOGY

Man will always seek to use technology to further himself while also using it to diminish the threat possessed by those around him. Often, innocent technologies can be used to create weapons or damaging effects in time of war. The crawler tractor was initially developed to assist in the preparation of fields for agriculture, but quickly became the critical component of the tank. Cellular phones and their networks were created to make communications easier; however, they can also be manipulated to create battlefield effects. To better understand the vulnerability of cellular phones in combat, one needs to examine a case study that details the key actions and effects of this capability. The 2014 Russian

invasion, and subsequent occupation, of eastern Ukraine is the best case study to explore this activity.

This case study is pertinent because it is the only one that illustrates the vulnerabilities of cellular phones on a large scale. The United States has manipulated the phones of individuals fighters, but not nearly to the scale of the Russians. The Russian military and its proxies have targeted entire units and spoofed applications to take advantage of unsuspecting users. The Chinese are manipulating data and cellular networks through their 5G technology; however, at this time, these resources have not been utilized in any armed conflict. The Islamic State and Al Qaeda also manipulated cellular communications, but these actions were on a far smaller scale than the Russians, and often were only used to recruit new members and conjure support throughout the world. These entities did not use cellular communications to gain any advantage in combat.

The use of a detailed case study will look at the conflict and allow a proper analysis of the various means and effects of cellular and smartphone manipulation in Ukraine. Furthermore, the Russian invasion of Ukraine is relevant because it shows what may happen to other countries on the border with Russia. The potential of this occurring to the United States military is significant since it is currently rotating Army Armored Brigade Combat Teams through Eastern Europe, in conjunction with the Infantry (Airborne) and Stryker Brigade Combat Teams stationed on the Continent, to train with partner forces. Working with these partner forces may place U.S. personnel in danger of mobile phone manipulation due to the proximity of Russian forces to training areas. It is also vital that U.S. personnel become fully aware of these vulnerabilities so they can better protect themselves and prepare partnered forces for Russian tactics, techniques, and procedures.

Furthermore, some partner forces may not have the necessary encrypted communications equipment. Due to this shortcoming, the Ukrainian military relied heavily upon personal phones to send reports and issue tactical commands. While the United States military is fortunate to have encrypted communications devices down to the squad and even individual soldier level, not every nation or partnered force has this luxury. Leaders within the United States military need to be aware of threats to their forces and to partner forces that may also rely on cellular communications.

## B. STRUCTURE

The thesis is structured as follows: Chapter II will give a technical background on the history and operation of cellular phones and networks. The chapter will also examine the operation and use of International Mobile Subscriber Identity Catchers. Chapter III is the Ukraine case study. This chapter will give a background to the Russian invasion and their development of the New Generation Warfare strategy. It will also cover each of the three vulnerabilities and how they were exploited during the conflict in Ukraine. Each vulnerability will conclude with an example affecting the United States military for added significance. Chapter IV will envision future threats enabled by mobile and smartphone use by the United States military using the vulnerabilities discussed in the previous chapter. After an examination of current and future threats, Chapter V will describe some prescriptive measures the United States military can adopt to mitigate these concerns. Mitigation measures will focus on the education and training of individual service members, U.S. military organizations, as well as allies and partner forces.

THIS PAGE INTENTIONALLY LEFT BLANK

# II. TECHNICAL BACKGROUND

## A. HISTORY OF MOBILE PHONES

A mobile phone is a communications device designed to be carried by a person and used while outside of a static environment. The idea of a mobile communications device is not new. What is commonly thought of today as a mobile phone was first developed during the Second World War. Soldiers utilized "handie talkies" to communicate between units at the company level and below.[1] These devices, like the phones of today, had vulnerabilities that the Germans and Japanese exploited to gain tactical intelligence.[2] After the war, technology was adapted to create mobile phones that could fit inside vehicles. These early devices were too large to be conveniently carried by a person, but could fit into vehicles with relative ease. In today's vernacular, "mobile phone" and "cell phone" are used synonymously.[3] However, the phrase "mobile phone" refers to a broad classification of devices that facilitate voice communications while moving. Cellular phones, which will be the subject of this chapter, use a networked infrastructure of antennae to send and receive messages.

The first cellular phone, Motorola's DynaTAC 800x, was invented in 1983. The phone was nearly a foot long, weighed 2 pounds, and had a battery life of about 30 minutes.[4] The first smartphone, IBM's Simon, was created in 1993. Simon was a phone, notepad, calendar, address book, had a stylus, provided email service, and utilized predictive typing on its touch screen.[5] Cellular phones were labeled "smart" when they gained the ability to connect to the internet. An examination of the history of the mobile

---

[1] Gil McElroy, "A Short History of the Handheld Transceiver," *QST* (January 2005): 45–50, https://web.archive.org/web/20060220092549/http://www2.arrl.org/qst/2005/01/0501047.pdf.

[2] Robert M. Clark, *Intelligence Collection* (Los Angeles, CA: SAGE, 2014), 96.

[3] Kelly, "Why Do We Use the Term Cellular Phone Instead of Mobile Phone?" Gizmodo, June 17, 2013, gizmodo.com/why-do-we-use-the-term-cellular-phone-instead-of-mobile-5840939.

[4] Arun Kumar et al., "Mobile Phones: History and Growth," *EPRA International Jouranl of Research and Development* 4, no. 3 (March 2019): 44–45, https://eprajournals.com/jpanel/upload/837pm_11.Arun%20Kumar%20S-3013-1.pdf.

[5] Kumar et al., "Mobile Phones: History and Growth," 46–47.

phone is interesting because it shows how far technology has developed in such a short period.

In less than thirty years, the smartphone has evolved and developed into a tool that many people cannot live without. In 2020, nearly 3.5 billion people, or almost a third of the Earth's population, own a smartphone.[6] The number of people using the internet from mobile devices has surpassed the number of people using desktops in 2016.[7] This trend is expected to continue. Most Americans no longer have landline phones. Cellular and smartphones have woven themselves into the fabric of everyday life. The same holds true within the military. Many service members are reliant on their phones for communications, research, entertainment, and relaxation. An understanding of cellular phones and their networks is essential to the study of the vulnerabilities introduced on the battlefield by these devices. The following description of cellular networks and components, the generations of mobile communication technology, and an introduction to International Mobile Subscriber Identity (IMSI) Catchers will assist in comprehending how phones are manipulated and the tools that execute these manipulations.

## B. CELLULAR NETWORK STRUCTURE

Cellular networks are made up of small areas called cells. Within each of these cells is an antenna which is controlled by a base station that has its own unique group of radio channels. However, a tower located at least two cells away from another can reuse the same channels.[8] The cells are hexagonal in shape to maximize the effective radius of each tower.[9] These cells are situated in clusters of seven (see Figure 1). This allows each cluster to work seamlessly with other clusters of seven cells to create a cellular communications

[6] Deyan G., "60 Revealing Statistics about Smarthpone Usage in 2020," Tech Jury, January 9, 2020, techjury.net/stats-about/smartphone-usage/#gref.

[7] Yoni Heisler, "Mobile Internet Usage Surpasses Desktop Usage for the First Time in History," BGR, November 22, 2016, bgr.com/2016/11/02/internet-usage-desktop-vs-mobile/.

[8] Oliver C. Ibe, *Fundamentals of Data Communication Networks* (Hoboken, NJ: Wiley, 2018), 256.

[9] Khaldoun Al Agha, Guy Pujolle, and Tara Ali-Yahiya, *Mobile and Wireless Networks*, vol. 2 (Hoboken, NJ: Wiley, 2016), 19, https://doi.org/10.1002/9781119007548.

network in a region.[10] It should be noted that to provide effective coverage, each cell is not a perfect hexagon due to topography and different propagation conditions.[11]

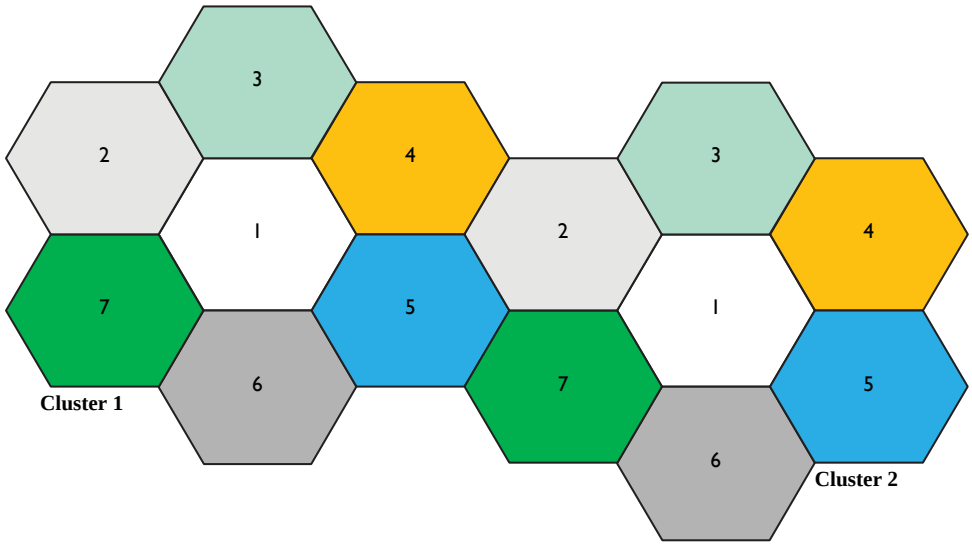



Figure 1. Illustration of Frequency Reuse in Two Adjacent Clusters[12]

Cellular phone networks consist of four components: 1) mobile station, 2) base station, 3) base station controller, and 4) mobile switching center.[13] The mobile station, or a mobile subscriber unit (MS), is the phone, tablet, or another device that is connected to the cellular network.[14] The MS then has a transceiver that transmits and receives radio transmission to and from a base station.

The base station (BS) is the tower within the center of a cell. Two different channels for traffic flow from the BS to the MS. The first is the control channel, which works to ensure the seamless transfer of information to maintain the connection through different

[10] Oliver C. Ibe, *Fundamentals of Data Communication Networks* (Hoboken, NJ: Wiley, 2017), 257.

[11] Al Agha, Pujolle, and Ali-Yahiya, *Mobile and Wireless Networks*, 19.

[12] Source: Ibe, *Fundamentals of Data Communication Networks*, 257.

[13] Ibe, 259.

[14] Ibe, 259.

cells. The second channel is used for the transport of voice, data, and other traffic.[15] Multiple base stations can be controlled by a Base Station Controller (BSC), which also acts as the interface for the BS and the Mobile Switching Center.

An important component of voice communications is the Public Switched Telephone Network (PSTN). The PSTN is the traditional circuit switch telephone network that links all of the world's telephone communication networks, made up of numerous switches that help to connect calls through landlines, microwave transmissions, cellular networks, communications satellites, and undersea telephone cables.[16] The PSTN is what allows most telephones to communicate with one another. For example, a call made from a satellite phone can be answered by a landline phone and vice versa. While the PSTN used to be made up of copper wires, it is now almost entirely digital and utilizes fiber optic cable.

The Mobile Switching Center (MSC) acts as the go-between from the cellular base station to the PSTN. In effect, the MSC acts as the interface with different networks within the PSTN (i.e., landline to cellular). However, the MSC is not just used in routing phone calls but also in conference calls, text messages, and faxes.[17] The MSC is also a critical component in an inter-BSC handover. When "a mobile device is approaching the edge of its cell, a BSC requests handover assistance from its MSC. The MSC then scans a list of adjacent cells and their corresponding BSCs and facilitates the handover to the appropriate BSC."[18] Another important job for the MSC is the handover of an MS to a different BS. As a phone moves closer to being out of range from its current base station, "it is important for the MSC to determine each phone's location to effectively facilitate routing communications between them."[19] To accomplish this, the MSC uses an extensive

15 Al Agha, Pujolle, and Ali-Yahiya, *Mobile and Wireless Networks*, 21.

16 Cameron Johnson, "What Is PSTN and How Does it Actually Work?" Nextiva, April 4, 2019, www.nextiva.com/blog/what-is-pstn.html.

17 "What Is a Mobile Switching Center (MSC)?" Techopedia, accessed May 3, 2020, www.techopedia.com/definition/8448/mobile-switching-center-msc.

18 Techopedia.

19 Techopedia.

"database known as the home location register (HLR), which stores relevant locations and other information for each mobile phone."[20] To prevent numerous search queries to the HLR, each MSC utilizes a Visitor Location Register (VLR) to cover the users currently roaming in the MSC location area. As will be described later, the data in these registers is an important source of information for IMSI Catchers, which use it to locate phones. This vulnerability is especially concerning to soldiers using phones on the battlefield. The entire cellular network and its components are illustrated in Figure 2.

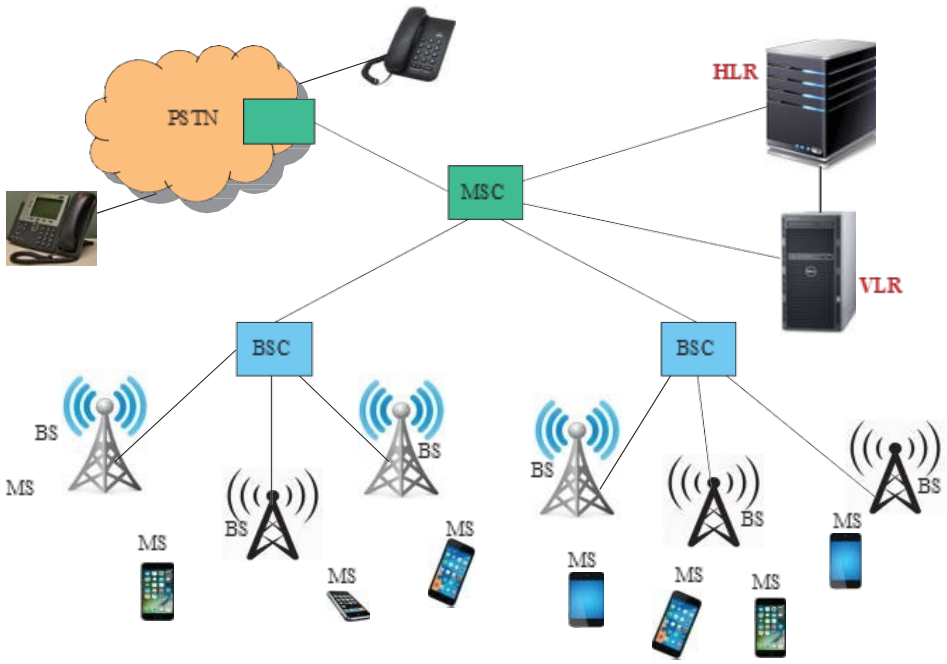



Figure 2. Architecture of Mobile Communication Networks[21]

## C. GENERATIONS OF MOBILE TECHNOLOGY

Five successive generations of mobile communications technology have been created. Each new generation offers improvements to the older generation. These improvements vary from network design to increased data rate and additional security. As

[20] Techopedia.

[21] Source: Ibe, *Fundamentals of Data Communication Networks,* 260.

of 2020, the world is on the cusp of utilizing Fifth Generation Mobile technology. However, the majority of the United States is still using Fourth Generation Technology. The following describes the five current generations of mobile technology.

### 1. First Generation Mobile Technology

The first generation of mobile technology (1G) was completely analog and only capable of voice services.[22] What differentiated 1G technology from earlier mobile communications networks, however, was its use of cellular technology. In the past, companies tried to make powerful base stations that could enable communication throughout its effective radius. The effective radius was about 50 miles and proved useful in metropolitan areas.[23] But, once a user left that area, he/she could no longer communicate. This shortcoming necessitated the development of multiple small frequency base stations—a cellular structure—which were found to be more effective in creating a mobile communications network. While 1G technology had good voice quality, its spectral efficiency, or the rate of transported information on a specific frequency, was low.

### 2. Second Generation Mobile Technology

Second generation (2G) cellular networks were primarily voice and secondary data networks. As opposed to the 1G network, the speed of these networks was also faster. The 1G PSTN data rate was 2.4kbps, while the 2G network's data rate 64 kbps.[24] The increased spectral efficiency, speed, is due to the abandonment of 1G analog technology and the shift to digital technology utilized in 2G. Two of the most used networks utilizing 2G technology were the Global System for Mobile Communications (GSM) and Code Division Multiple Access (CDMA). These two different network types were used by different providers and utilized MS that were incompatible with the other network (i.e., a GSM phone could not be used in a CDMA covered area). One of the most significant weaknesses of this technology is the lack of authentication between the BS and MS. A MS, or phone, must

[22] Al Agha, Pujolle, and Ali-Yahiya, *Mobile and Wireless Networks*, 2.

[23] Ibe, *Fundamentals of Data Communication Networks*, 262.

[24] Ibe, 262–63.

identify itself to the BS, or tower, but not vice versa.[25] The lack of authentication opens 2G technology to the threat of BS spoofing.

### 3. Third Generation Mobile Technology

Networks that comply with the specifications outlined in the International Mobile Telecommunications 2000 agreement by the International Telecommunications Union are considered third generation (3G) mobile networks.[26] 3G provided transmission speeds of 2MB/s for stationary or walking users and 348KB/s for moving vehicles.[27] This technology allowed advanced capabilities such as "Global Positioning System (GPS), location-based services, video on demand, and video conferencing."[28] 3G Technology also allowed MS to authenticate the network they are connecting to as a means to prevent cell tower spoofing.

### 4. Fourth Generation Mobile Technology

Fourth Generation Mobile Technology is completely Internet Protocol (IP) driven.[29] The speeds of 4G are significantly faster and allow the user to enjoy better voice quality, faster downloads, higher streaming speeds, and less buffering. Data rates for 4G in moving vehicles are 100MB/s and 1GB/s when stationary.[30]

### 5. Fifth Generation Mobile Technology

The latest generation of mobile communications networks is still in development at the time of writing. However, this technology is expected to move data faster and allow significantly more devices to connect to the network. 5G is designed to meet the challenges

---

[25] Joseph Ooi, "IMSI Catchers and Mobile Security" (capstone thesis, University of Pennsylvania, 2015), 8, https://www.cis.upenn.edu/wp-content/uploads/2019/08/EAS499Honors-IMSICatchersandMobileSecurity-V18F.pdf.

[26] Ooi, "IMSI Catchers and Mobile Security," 9.

[27] Ooi, 9.

[28] Ooi, 9.

[29] "Generations of Mobile Networks: Explained," Just Ask Gemalto, August 2, 2018, www.justaskgemalto.com/us/ generations -mobile-networks-explained/.

[30] Ooi, "IMSI Catchers and Mobile Security," 9.

of the Internet of Things (IoT).[31] As more and more appliances and devices connect to the IoT, a new, more extensive, faster, and more flexible network is needed to ensure satisfactory performance for the end-user.

## D. INTERNATIONAL MOBILE SUBSCRIBER IDENTITY CATCHERS

Creating devices to deceive an adversary are as old as war itself. The best example of this is the Trojan Horse. During the war against the Trojans, the Greeks built a giant wooden horse disguised to look like a gift to the Trojans, but in actuality, it was full of soldiers. When the Trojans brought the gift into the gates of Troy, the deception was revealed, and Greek soldiers poured out of the horse and gained entry to the fortress city of Troy with relative ease. An International Mobile Subscriber Identity (IMSI) Catcher acts in a similar vein, in terms of its deceptive capability.

In short, an IMSI Catcher acts as a fake base station or cellular tower. "IMSI catchers use a 'man-in-the-middle' attack, simultaneously posing as the fake mobile phone to the real base station and as the fake base station to the real mobile phone."[32] This is illustrated in Figure 3. Like the "Greeks bearing gifts," it deceives phones by making it believe the IMSI catcher is a base station with the strongest signal in the area. This capability allows the phone to disconnect from a legitimate tower and reconnect automatically with the IMSI catcher or fake base station. As discussed earlier, 2G technology does not need the tower or BS to authenticate itself to the phone, MS. Only the phone has to authenticate itself to the tower. This is rectified in 3G when both the tower and the phone have to authenticate with one another. Currently, all phones are backward compatible with older-generation infrastructure.[33] Thus, a 4G phone can work on a 2G network to ensure seamless service for the user. Unfortunately, most IMSI catchers work on the 2G network. The phones, regardless of generation, having been deceived go into the 2G mode, no longer expect authentication from the tower, and connect to the IMSI catcher.

---

[31] Ibe, *Fundamentals of Data Communication Networks,* 271.

[32] Ooi, "IMSI Catchers and Mobile Security," 10.

[33] Adrian Dabrowski et al., "IMSI—Catch Me If You Can: IMSI-Catcher-Catchers," *Proceedings of the 30th Annual Computer Security Applications Conference* (2014): 246–55, https://doi.org/10.1145/2664243.2664272.

The IMSI is a unique number stored in the Subscriber Identity Module, or SIM card, inside each cellular phone, or MS.[34] This number "is used to acquire the details of the mobile [device] in the […] HLR or the […] VLR."[35] With this information, the IMSI Catcher can locate phones as well as identify the traffic in its vicinity and then target that traffic for interception and analysis.[36] These devices can target anyone in a variety of settings, to include soldiers on the battlefield.

IMSI Catchers have the ability to manipulate cell phones and gather significant amounts of information from them. While the basic catcher can be used to locate a phone's user, more advanced models and upgrades can be used to eavesdrop on the user's calls, record calls, intercept and redirect SMS, and, most strikingly, retrieve files from the phone. For example, the most well-known commercially developed IMSI Catcher, the Stingray, can be upgraded by the Harris Corporation with a "FishHawk" system to eavesdrop on calls and the "Porpoise" system to read text messages.[37] These add-ons make IMSI catchers very effective intelligence gathering tools for government, military, and criminal elements.

Another unique ability of the IMSI catcher is its ability to send mass text messages. Using the same process of deception described earlier, the catcher acts as a cellular tower and attracts phones to connect with it. Once the phones have authenticated themselves to the catcher, it "sends an SMS message to the user device using a spoofed phone number. This action can be repeated multiple times."[38] The spoofed phone number can be from a legitimate business or any other number to make the sent message seem more trustworthy. In China, these illegal devices are not used only for advertising; some nefarious groups use the mass texting ability of fake base stations in phishing attacks to get the personal

---

[34] "What Is International Mobile Subscriber Identity (IMSI)?" Techopedia," last updated November 15, 2016, www.techopedia.com/definition/5067/international-mobile-subscriber-identity-imsi.

[35] Techpodeia.com.

[36] Ooi, "IMSI Catchers and Mobile Security," 10.

[37] Ryan Gallagher, "Meet the Machines That Steal Your Phone's Data," Ars Technica, September 25, 2013, arstechnica.com/tech-policy/2013/09/meet-the-machines-that-steal-your-phones-data/.

[38] Zhenhua Li et al., "FBS-Radar: Uncovering Fake Base Stations at Scale in the Wild," paper presented at the NDSS Symposium 2017, 4, https://doi.org/10.14722/ndss.2017.23098.

information of their victims.[39] After sending the message, the catcher needs to cut off from the phone to prevent the user from realizing it has been connected to a fake base station. The catcher ends the connection by lowering its signal strength, changing its base station ID, or ending the signal.[40] This allows the user's device to reconnect to a legitimate base station.

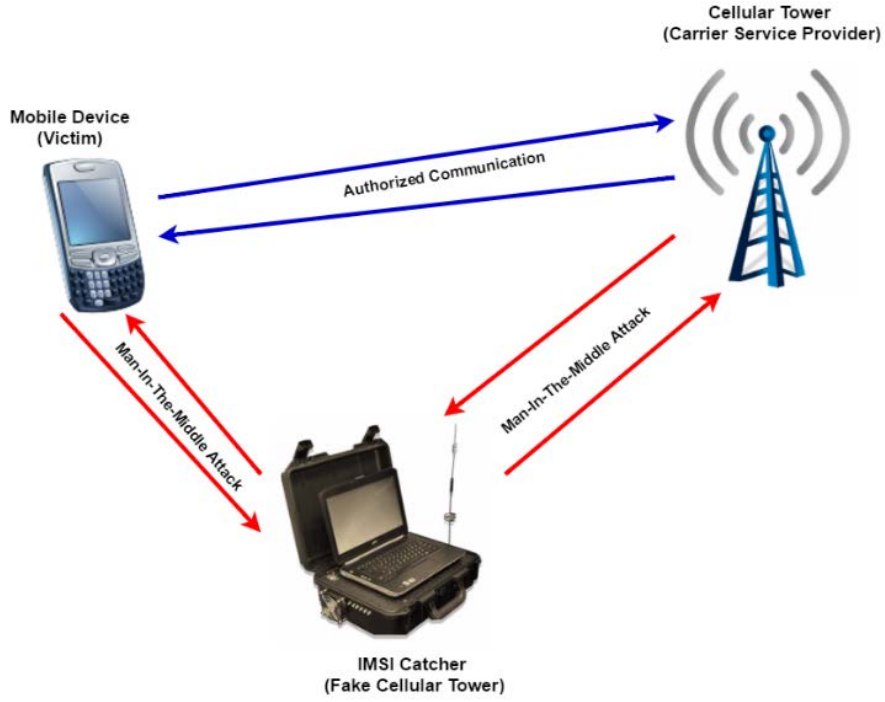



Figure 3. Diagram of IMSI Catcher Use[41]

## E. HISTORY OF IMSI CATCHER USE

The first IMSI Catcher was created as early as 1993.[42] These early pieces of technology were large and, at the time, very cost-prohibitive. However, in 2010, Chris Paget presented a homemade IMSI catcher he built for about $1,500 at the hacker

[39] Russell Brandom, "Phony Cell Towers Are the Next Big Security Risk," The Verge, September 18, 2014, www.theverge.com/2014/9/18/6394391/phony-cell-towers-are-the-next-big-security-risk.

[40] Li et al., "FBS-Radar," 4.

[41] "IMSI Catcher Detector: Stingray Surveillance Detection Services: USA," COMSEC, December 21, 2018. https://comsecllc.com/imsi-catcher-detector/.

[42] Dabrowski et al., "IMSI—Catch Me If You Can," 246–47.

exposition, DEFCON.[43] The devices were initially marketed to Law Enforcement entities to track the location of suspects through the use of their cellular phones.[44] The United States Marshals, who are known for high-risk fugitive apprehension, pioneered the use of IMSI Catchers to assist in the location and arrest of criminals.[45] The Marshal Service operated several Cessna light aircraft with powerful IMSI Catchers. The combination of rapid movement from the aircraft, and the powerful scanner of the IMSI catcher, meant the Marshals Service could search a large metropolitan area for certain cell phones that were known to be used by the criminals they were targeting. The unfortunate consequence was that thousands of other innocent Americans were having their cell phones intercepted by the law enforcement agency. Within the United States, there is some debate on the legality of law enforcement entities to use IMSI catchers in regard to the illegal search of innocent citizens' phones.[46]

Militaries also utilize IMSI Catchers. The United States military employed IMSI catchers to locate terrorists in both Iraq and Afghanistan.[47] The Israelis may have also used these devices to send messages to residents in Gaza. To prevent civilian casualties and collateral damage, the Israeli Defense Force (IDF) sends texts, phone calls, and leaflets to warn civilians about upcoming strikes and the danger of being close to Hamas weapons and facilities. An official Israeli Defense Force website, aimed at illustrating the ways Israel prevents collateral damage in Gaza, states, "As part of its efforts to minimize civilian casualties in Gaza, the IDF makes phone calls and sends text messages to civilians residing in buildings designated for an attack."[48] Presumably, the IDF utilized an IMSI catcher to

---

[43] Ooi, "IMSI Catchers and Mobile Security," 4.

[44] Ooi, "IMSI Catchers and Mobile Security," 10.

[45] Devlin Barrett, "Americans' Cellphones Targeted in Secret U.S. Spy Program," *Wall Street Journal*, November 14, 2014, www.wsj.com/articles/americans-cellphones-targeted-in-secret-u-s-spy-program-1415917533.

[46] "Stingray Tracking Devices," American Civil Liberties Union, accessed May 3, 2020, www.aclu.org/issues/privacy-technology/surveillance-technologies/stingray-tracking-devices.

[47] Sean Naylor, *Relentless Strike: The Secret History of Joint Special Operations Command* (New York, NY: St. Martin's, 2015), 263–64.

[48] "How Is the IDF Minimizing Harm to Civilians in Gaza?" IDF, July 16, 2014, www.idf.il/en/articles/hamas/how-is-the-idf-minimizing-harm-to-civilians-in-gaza/.

disseminate text messages to the greatest number of people in their targeted area. Conversely, Hamas has also sent text messages to the Israeli population. In response to an Israeli offensive into Gaza in late 2008, Hamas sent a message threatening rocket attack reprisals into cities in Israel.[49] The IDF and Hamas text battle is unique as it shows cell phone use against state and non-state actors. The War in Ukraine shows the more widespread use of IMSI Catchers and their ability to send mass text messages to cellular phones.

Much like the Israelis, Hamas, and Chinese criminals, the Russians have used IMSI catchers to send text messages to cellular phones as a means to spread propaganda. Going a step further, the Russians have employed drones to propagate their text message campaign by impersonating cell phone towers. This electronic warfare system is called LEER 3 and consists of three unmanned aerial vehicles (UAVs) and a mobile command center (see Figure 4). The UAVs' "primary mission is to suppress cellular communication towers. […] Having jammed the base stations, the old Orlan-10 UAVs were able to send instant messages to subscribers under certain conditions […] They 'jam' base stations and take their place, while becoming virtual cellular stations."[50] While not explicitly stating it, the Russians have produced flying IMSI catchers to jam enemy communications and send messages. These devices, like the IMSI catchers described earlier, can also be used to locate cell phone users. LEER 3 systems can also drop disposable jammers on the ground.[51] In Syria, Russia used the LEER 3 to alert Syrian civilians of humanitarian assistance centers and evacuation routes, despite the cellular network of the region being destroyed. By controlling the cellular architecture, the Russians have gained a significant advantage in controlling the information environment and influencing Ukrainian soldiers with ease.

---

[49] Ali Waked, "Hamas Sends Text Messages to Israeli Cell Phones." Ynetnews, June 14, 2011, www.ynetnews.com/articles/0,7340,L-3648799,00.html.

[50] Foreign Military Studies Office, "Russia's UAV Virtual Cellular Communication Tower," *OE Watch* 7 no. 2 (March 2017): 54.

[51] Foreign Military Studies Office, "Counter UAV Tactics and the 'Leer-3' Electronic Warfare System," *OE Watch* 7, no. 7 (August 2017): 3.

Figure 4. Leer 3 System with Command and Control Truck and Orlan-10 UAV[52]

Multiple vectors exist to compromise the user of a cellular phone. The infrastructure of the network, applications downloaded to phones, and the hardware installed in phones can all create vulnerabilities. This thesis will focus on the vulnerability of phones as vehicles for propaganda, targets of cyberspace exploitation, and OPSEC violations due to misuse by the user. The battlefield of Ukraine will exhibit these vulnerabilities clearly and show the direct battlefield effects these devices have had upon the combatants. The vulnerability of cellular phones shows the lack of understanding by the user as well as the lack of security in the network and the devices themselves.

[52] Source: "Russian Leer-3 EW System Revealed in Donbas," Inform Napalm, September 25, 2016, informnapalm.org/en/russian-leer-3wf-donbas/.

THIS PAGE INTENTIONALLY LEFT BLANK

# III. UKRAINIAN CASE STUDY

Ivan, a soldier in the Ukrainian 10th Mountain Assault Brigade, had been in the same battle position for well over a month. He had deployed to Eastern Ukraine for "Anti-Terrorism Operations" after the Russian invasion of Donbass. He had become accustomed to the daily mortar barrage at about 10 AM, and had gotten used to the rainy and cloudy days and chilly nights. His commander had finally acquired a night vision device to make sentry duty at night easier, but its novelty soon wore off. Recently, the Russian backed separatists seemed to have calmed down. Despite the mortar barrage in the late morning, there were no other attacks. Previously, the two sides conducted dismounted patrols within the area between the lines which often resulted in sporadic gunfights and occasional artillery strikes.

Just as Ivan was slipping into a daydream about his family back home, he felt his phone vibrate. "Speak of the devil," he thought, as he grabbed the phone from the shoulder pocket on his camouflage parka. He took it out of the plastic sandwich bag that protected it from the rain. The phone had a cracked screen, but he could still watch movies and navigate his apps. Ivan had received a text message, but it was not from whom he had hoped. "You have been charged 1000 hryvnia for supporting the Anti-Terrorism Operations," the text stated. He sighed. It was another message from the Russians. A couple of days ago he had received a more-sinister message telling him, "The same winter that ended the Nazis is coming for you." Most of the time, Ivan and his squad laughed about these messages. However, as the days went on and the time away from home compounded, Ivan started to have doubts about why he was at the front and what was happening with his family. The messages, in conjunction with low pay, mediocre food, and spartan living conditions, were beginning to affect him and the morale of his unit.

The scenario depicted above is realistic for members of the Ukrainian Army. The New Generation Warfare strategy employed by the Russians and their allied forces has emphasized operations in the information environment. Resulting in their ability to use weaknesses within cellular phones to target, disrupt, and destroy the Ukrainian forces that

oppose them. The cellular phone—a device that is so important to humans in the civilian world—can become their undoing in the tactical arena.

This chapter aims to illustrate, through the context of the 2014 Russian invasion and subsequent occupation of Ukraine, the vulnerabilities of cellular and smartphone use on the battlefield. The vulnerabilities that are created by using cellular phones on the battlefield include: phones being used as vehicles for propaganda by the enemy, as targets of cyberspace exploitation by the enemy, and as an OPSEC concern that the enemy can use as a source of intelligence. A background to the conflict will assist the reader in understanding the combatants and their reasons for fighting. Next, an overview of Russian New Generation Warfare (NGW) and its use of Information Warfare (IW) will be examined to show how the Russians view the information environment and look for ways to exploit it. Then, each vulnerability will be discussed, and an example from Ukraine will be utilized to illustrate how the phone was used to cause effects on the battlefield. Finally, an example of each cell phone vulnerability involving the United States will also be described to emphasize the susceptibility within the United States military. The conflict in Ukraine provides an interesting case study that reveals cell phone vulnerabilities on the battlefield. Furthermore, it illustrates some of the capabilities the Russians can bring to bear in conflict with other nations or irregular forces.

## A. HISTORY OF CONFLICT

From Turks to Tartars to Cossacks to Little Green Men, Ukraine has been a contentious region with a conflicted past. The main source of this disagreement is attributed to the Crimean Peninsula located south of Ukraine. Crimea holds a strategic position in the Black Sea as ports in this area can utilize the Bosporus sea lane through Istanbul to gain access to the Mediterranean and, eventually, the oceans of the world. For centuries, people have found Crimea to be an important piece of territory and worthy of fighting over for control.

After the Bolshevik Revolution in 1920, Ukraine was given its independence, but Crimea remained a part of Russia.[53] After the Second World War, many of the minorities, including Ukrainians, were deported from Crimea due to accusations of collaborating with the Nazis. In 1954 Crimea was given to Ukraine by Soviet leader Nikita Khrushchev to simplify economic, political, and administrative concerns.[54] This move was not popular within the populations of Crimea or Russia. The fall of the Soviet Union exacerbated these perceptions and caused more conflict.

Crimea sought to become an independent state from Ukraine. In 1992, Crimea created its own constitution and declared itself the "sovereign state of the Republic of Crimea," despite having its independence referendum canceled.[55] The region remained in limbo. In 1995 the Ukrainian Parliament abolished Crimea's 1992 Constitution.[56] Kyiv accepted a final, much weaker Crimean Constitution in 1998. The new constitution gave Crimea few rights and allowed them to make only small local law changes. The Ukrainian government attempted to force a linguistic and cultural "Ukrainification" program among the Crimean people.[57] The unsuccessful program only provoked a greater hope of independence on Crimea's part and a deepening resentment of Ukraine.

Since the fall of the Soviet Union, the Russians have viewed the expansion of the North Atlantic Treaty Organization (NATO) as a threat. Many wondered if NATO would continue to exist as an alliance after its sole threat was defeated with the collapse of the Soviet Union. The opposite occurred, and NATO expanded. Former Soviet satellite states joined NATO as a sign of support for Western Europe. NATO was established in 1949 with twelve original members, four more joined before the collapse of the Soviet Union.[58]

---

[53] Colby Howard and Ruslan Pukhov (eds.), *Brothers Armed: Military Aspects of the Crisis in Ukraine*, 2nd ed. (Minneapolis, MN: East View Press, 2015), 2.

[54] Howard and Pukhov, *Brothers Armed*, 4–5.

[55] Howard and Pukhov, 9.

[56] Howard and Pukhov, 13.

[57] Howard and Pukhov, 14–15.

[58] "Member Countries," NATO, June 9, 2017, www.nato.int/cps/en/natohq/topics_52044.htm.

Since the end of the Cold War, NATO has grown to include thirteen more countries, all of which were former Soviet satellites.

Russia, therefore, has sought to end NATO enlargement. It has protested every country's adoption into NATO since the end of the Cold War. "In April 2008, NATO promised membership to Georgia and Ukraine at the Bucharest summit, but a membership plan was not offered."[59] Several months later, in August 2008, Russia invaded Georgia under "the pretext of defending the breakaway regions of South Ossetia and Abkhazia."[60] These regions later declared their independence from Georgia; however, "Russia is one of the few countries in the world to recognize this [pronouncement]."[61]

There was also a Russian response to Ukrainian efforts to join NATO and the European Union. Russians pressured the Ukrainian leadership to remain at their side instead of joining the west. "The demonstrations which began in Kyiv, known as the Maidan Protests, in November 2013 were born out of Ukrainians' desire for a closer relationship with the European Union, and their frustration when former President Yanukovych halted progress toward that goal as a result of Russian pressure."[62] Yanukovych was from the Donbass region of eastern Ukraine, which is heavily influenced by Russia. He aimed to strengthen relations with Russia, which instigated a growing series of civil demonstrations throughout Ukraine, the Maidan Protests.[63] The protestors' demands included a government of national unity, an end of government corruption, early presidential elections, and an end to violent government actions against demonstrators.[64] These protests ended with the removal of Yanukovych on 22 February 2014.[65] The

[59] Madeline Roache, "Inside the Complicated Relationship between Russia and NATO," *Time*, April 4, 2019, time.com/5564207/russia-nato-relationship/.

[60] Roache, "Inside the Complicated Relationship between Russia and NATO."

[61] Roache.

[62] "Russia Relations: The Facts," NATO, July 9, 2016, www.nato.int/cps/en/natohq/topics_111767.htm#cl410.

[63] Vladimir Sazonov and Holger Mölder, "Why Did Russia Attack Ukraine?" *ENDC Occasional Papers* 6 (2017): 29.

[64] NATO, "Russia Relations."

[65] Sazonov and Mölder, "Why Did Russia Attack Ukraine?," 29.

Russians saw this as a threat to their influence in the region and an opportunity to secure access to the Black Sea by invading Crimea. The continued unrest in Ukraine sparked another opportunity for Russia to invade eastern Ukraine. This action, like a similar incursion into Georgia eight years before, destabilized the borders of those countries; border conflict is a disqualifier for NATO acceptance.[66] While both countries aspire to become NATO members, they cannot due to their border disputes with Russia.

The valuable naval assets of the Black Sea Fleet proved to be another point of contention for Ukraine and Russia. Upon the collapse of the Soviet Union, both Russia and Ukraine claimed possession of the fleet and its military assets.[67] Russia eventually was allowed to claim 81.7% of the vessels, continue to keep of force 25,000 service personnel stationed in Crimea, and the stipulation that any military equipment introduced or removed needed the approval of Ukraine. This agreement was to last twenty years and would have been up for review in 2017.

Russia's goal is to maintain an "uncontested and exclusive sphere of influence in the territory that once formed the Soviet Union."[68] To accomplish this aim, the Russians leverage the weaknesses in their adversaries and counter strengths at a level below the threshold of war in order to achieve their aspirations.[69]One of the most effective tools is to utilize information warfare.

## B. RUSSIA AND INFORMATION WARFARE

The Invasion of Ukraine has provided a unique laboratory for Russia to experiment and test many of its new capabilities, stratagems, and techniques. The success of this operation should not surprise a student of modern Russian military history. Instead, it shows a natural progression from operations in Chechnya and Georgia. The current Russian strategy is known by many names: The Gerasimov Doctrine, Hybrid Warfare, Non-linear

66 "Study on NATO Enlargement," NATO, November 5, 2008, www.nato.int/cps/en/natohq/official_texts_24733.htm.

67 Howard and Pukhov, *Brothers Armed*, 17–18.

68 Robert Person, "Russian Grand Strategy in the 21st Century," in *Russian Strategic Intention: A Strategic Multilayer Assessment (SMA) White Paper*, ed. Nicole Peterson (Boston, MA: NSI, May 2019), 7.

69 Person, "Russian Grand Strategy in the 21st Century," 9.

Warfare, or as the Russians themselves call it, New Generation Warfare.[70] The Russians no longer see a difference between war and peace. Everything to them is a state of conflict. Because of this broad view, NGW encompasses all the elements of state power and incorporates military might with non-military means. According to Molly K. Mckew, Russia's NGW is "waged on all fronts with a range of actors and tools—for example, hackers, media, businessmen, leaks and, yes, fake news, as well as conventional and asymmetric military means. Thanks to the internet and social media, […] upending the domestic affairs of nations with information alone—are now plausible."[71] The man credited with creating this strategy of Russian warfare is General Valery Gerasimov, who authored, "The Value of Science in Prediction" in February 2013.[72] He is Russia's chief of the General Staff, which is comparable to the U.S. chairman of the Joint Chiefs of Staff.[73] The Russian military views this new strategy as a direct counter to the type of threat they perceive from the West and have taken significant steps to ensure its military is prepared to fight and prevail in this type of conflict.

The Russian use of IW is perhaps their most effective weapon. Mark Galeotti believes, "The Russian view of modern war is based on the idea that the main battlescape is the mind and, as a result, new-generation wars are to be dominated by information and psychological warfare."[74] The Russians understand the importance of the information environment and information dominance. IW can have a far greater effect on the enemy than traditional kinetic operations.

---

[70] Jānis Bērziņš, "Russia's New Generation Warfare in Ukraine: Implications for Latvian Defense Policy" (policy paper, National Defence Academy of Latvia Center for Security and Strategic Research 2014), 4.

[71] Molly K. McKew, "The Gerasimov Doctrine: It's Russia's New Chaos Theory of Political Warfare. And It's Probably Being Used on You," *POLITICO*, September 10, 2017, https://www.politico.eu/article/new-battles-cyberwarfare-russia/.

[72] Mark Galeotti, "The 'Gerasimov Doctrine' and Russian Non-linear War," In Moscow's Shadows, September 17, 2017, inmoscowsshadows.wordpress.com/2014/07/06/the-gerasimov-doctrine-and-russian-non-linear-war/.

[73] McKew, "The Gerasimov Doctrine."

[74] Mark Galeotti, *Russian Political War: Moving beyond the Hybrid*, 1st ed. (Abingdon, UK: Routledge, 2019), 43.

The Russians have proven to be very capable and confident in their ability to exploit and manipulate the information environment. Understanding the manipulation of the information environment is not a standalone operation; the Russians incorporate this strategy into all operations, including combined arms maneuver. The synchronization of Electronic Warfare, Information Operations, Cyber Operations, Psychological Operations, and kinetic actions into one combined threat is a hallmark of the Russian military. Many Russian senior military leaders believe "information is 'not just an addition to firepower, attack, manoeuvre, but transforms and unites all of these.'"[75] The actions of Russia during the Ukrainian Campaign illustrate this capability well through the exploitation of cellular and smartphone use on the battlefield.

## C. MEDIUM OF PROPAGANDA

The use of "pinpoint propaganda" represents perhaps one of the most sinister tactics to emerge from the war in Ukraine.[76] This is an influence operation where a soldier is sent a message directly from the enemy. The most common method for sending this information is by text message on the soldier's mobile phone. Since the conflict began, Ukrainian soldiers have been receiving targeted text messages from pro-Russia Militias or the Russian military (see Figure 5). These messages include: "*UAFers [Ukrainian Armed Forces], you're just [nothing but] meat for your commanders; UAF [Ukrainian Armed Forces] soldier! You'll be found [they'll find your body] when the snow melts, ATO [Anti-Terrorism Operation] fighter; This Winter is [looking like the one that hit] the Germans near Stalingrad.*"[77] Messages like this have the potential to decrease morale within the Ukrainian Military. More insidious accounts include text messages sent to the families of

[75] Margarita L. Jaitner, "Russian Information Warfare: Lessons from Ukraine," in *Cyber War in Perspective: Russian Aggression against Ukraine*, ed. Kenneth Greers (Tallinn: NATO Cooperative Cyber Defense Centre of Excellence, 2015).

[76] Raphael Satter, "Ukraine Soldiers Bombarded by 'Pinpoint Propaganda' Texts," Associated Press, May 11, 2017, apnews.com/9a564a5f64e847d1a50938035ea64b8f/Sinister-text-messages-reveal-high-tech-front-in-Ukraine-war.

[77] Daniel Brown, "Russian-Backed Separatists Are Using Terrifying Text Messages to Shock Adversaries—And It's Changing the Face of Warfare," *Business Insider*, August 14, 2018, www.businessinsider.com/russians-use-creepy-text-messages-scare-ukrainians-changing-warfare-2018-8.

Ukrainian soldiers, urging them to give up and go home.[78] Most soldiers expect the hardships of the battlefield and are trained to be resilient in these conditions. Family members are less prepared for the effects of the battlefield. For family members to receive direct propaganda attacks must have had a tremendous impact on the morale of soldiers and decreased the motivation of the civilian population as well.

The use of propaganda, psychological operations, and Military Information Support Operations (MISO) has occurred for centuries, and the conflict in Ukraine is no different. Russian leadership "invests significant resources in both foreign and domestic propaganda and places a premium on transmitting […] consistent, self-reinforcing narratives regarding its desires and redlines, whether on Ukraine, Syria, or with the United States."[79] What makes this action unique is the use of phones as a medium for enemy propaganda. At the tactical level, psychological warfare aimed at causing fear or at building a divide between the soldier and the government or home front is called counterforce.[80] In the past, leaflets and loudspeakers infected groups with propaganda; there have been few cases where an individual becomes the target. In 1995 Martin Libicki predicted a "great shift in counterforce psychological operations would come when information technology permits broadcast of threats or resentment-provoking information to *individual* opposing troops."[81] The necessary technology is now here. Text messages allow the user to tailor the message to an individual unit or even a particular soldier.[82]

---

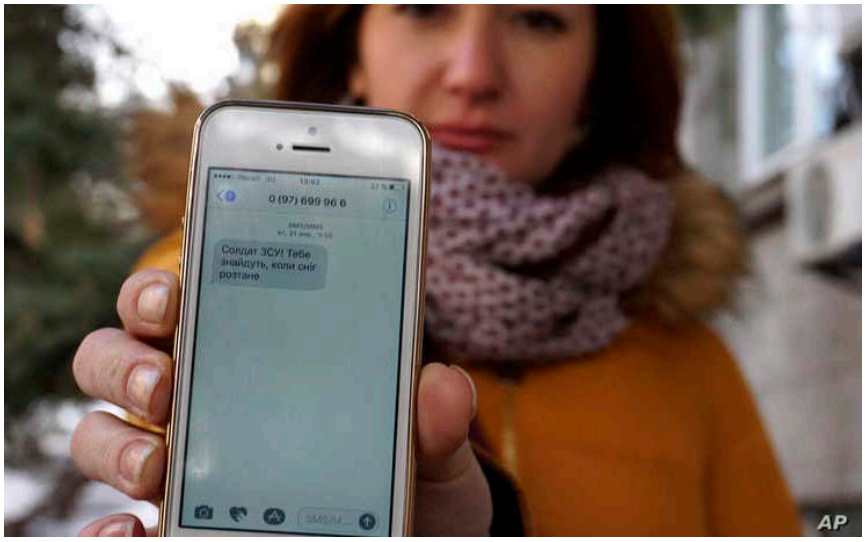
78 Aaron Brantly, "A Bear of a Problem: Russian Special Forces Perfecting Their Cyber Capabilities," Association of the United States Army, November 28, 2018, www.ausa.org/articles/bear-problem-russian-special-forces-perfecting-their-cyber-capabilities.

79 Office of the Director of National Intelligence, "Background to 'Assessing Russian Activities and Intentions in Recent U.S. Elections': The Analytic Process and Cyber Incident Attribution" (Washington, DC: National Intelligence Council, 2017), i.

80 Martin C. Libicki, *What Is Information Warfare?* (Washington, DC: National Defense University, Institute for National Strategic Studies, 1995), 39.

81 Libicki, *What Is Information Warfare?*, 40.

82 Keir Giles, *The Next Phase of Russian Information Warfare* (Riga, Latvia: NATO Strategic Communications Centre of Excellence, 2016), https://www.stratcomcoe.org/next-phase-russian-information-warfare-keir-giles.




Television reporter Julia Kirienko holding her phone with a text message she received while reporting from the conflict area. The text reads, "Ukrainian Soldier, They'll find your body when the snow melts."

Figure 5. Russian Text Message[83]

A collection of these text messages has been gathered by Raphael Satter, a reporter for Reuters News Agency.[84] The collection includes forty-two instances of propaganda text messages. Satter's dataset consists of the date, time, location, sent phone number, the original text in Cyrillic, and a translated version of the message in English. Unfortunately, this dataset is not complete, and some information such as the date, time, and location was missing for of some of the included text messages. This data combined with the location of attacks in eastern Ukraine, can give a better picture of who and where the Russians were targeting Ukrainians with their text message propaganda campaign.

The Uppsala Conflict Data Program (UCDP) dataset on Ukraine shows where a majority of the kinetic activity in Ukraine occurred. The UCDP "is the world's main provider of data on organized violence […]. Its definition of armed conflict has become the global standard of how conflicts are systematically defined and studied. UCDP

83 Source: "Sinister Text Messages Reveal High-Tech Front in Ukraine War," Voice of America, May 11, 2017, www.voanews.com/europe/sinister-text-messages-reveal-high-tech-front-ukraine-war.

84 Raphael Satter, "'You're Just Meat'—Ukrainian Soldiers Get Chilling Texts," Associated Press, May 11, 2017, apnews.com/1096d53b7e5a4a9682d6b434021fb2f8.

produces high-quality data, which are systematically collected, have global coverage, are comparable across cases and countries, and have long time series which are updated annually."[85] The attached graphics were created using the tools located in the free and open-source Quantum Geographic Information System (QGIS) visualization software. Figure 6 depicts the country of Ukraine and, in purple, the significant activities (SIGACTs) that have taken place in the country from 2014 to 2018. One can see from the map that a majority of the action has taken place in an area of eastern Ukraine called Donbass. This area consists of the provinces of Luhansk and Donetsk that border Russia.

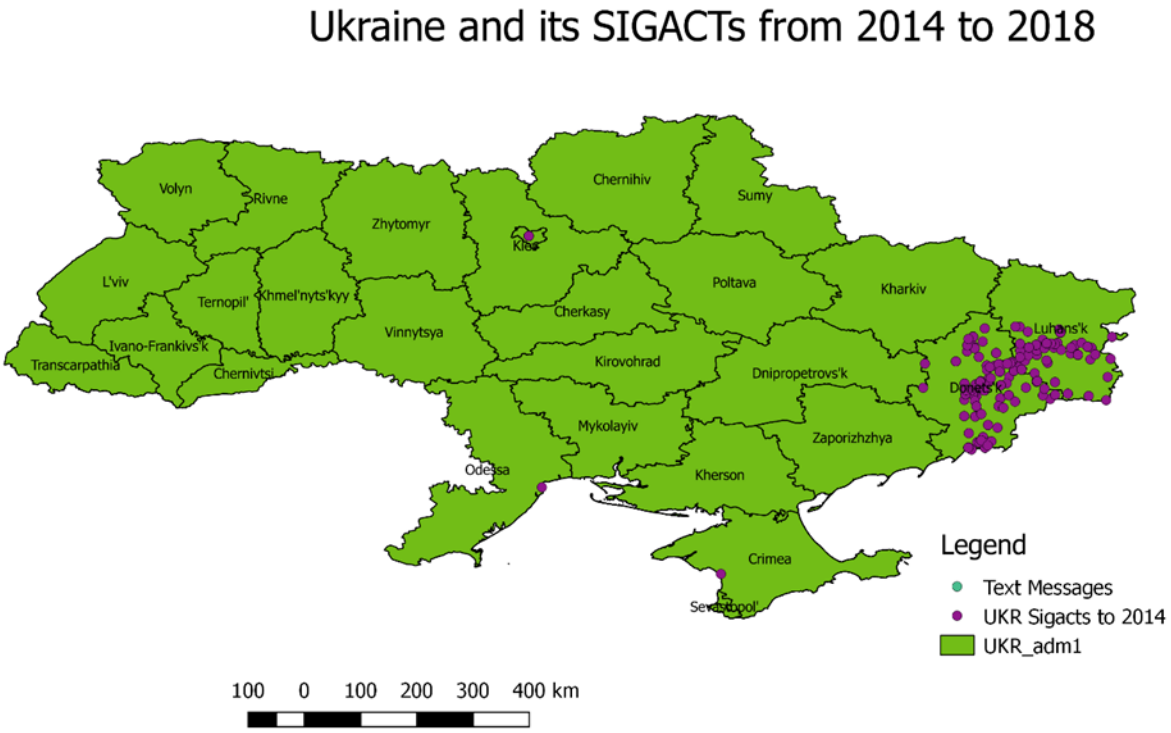



Figure 6. Map of Ukraine Showing the Location of SIGACTs from 2014 to 2018[86]

85 "About UCDP," Uppsala Universitet, accessed May 3, 2020, www.pcr.uu.se/research/ucdp/about-ucdp/.

86 Adapted from "Ukraine," UCDP, accessed May 11, 2020, https://ucdp.uu.se/country/369.

While there were also SIGACTs in Kyiv, Odessa, and Crimea depicted on the graphic, this thesis assumes that they are not salient to this analysis since they did not occur during times of combat. These data points represent protests, which are also a part of the UCPD dataset. The author believes the data point in Kyiv was in reference to the protests in February of 2014 that resulted in the ousting of President Viktor Yanukovych and the overthrow of the Ukrainian Government. There were similar protests in Odessa from January to May of 2014. The Crimea event is from the Russian annexation of territory in late February and early March of 2014. The majority of activity in the east stems from the Russian invasion. Russian supported separatists and Russian forces fighting against the Ukrainian Army and some militia forces are responsible for the remainder of the activity.

Figure 7 shows a close up of the Donbass conflict region, its SIGACTs, and the location of text messages received by Ukrainians based on Satter's dataset. The most significant aspect of this information is how the text message locations line up directly with the thickest belt of SIGACTs in Eastern Ukraine. The Russians have become quite proficient at combining the functions of information, movement and maneuver, and fires to make military operations more successful. Control of the information environment has made Russian military action more effective. One of the techniques used by the Russians to gain this control of the information environment is to manipulate the inherent vulnerabilities of cellular phones.

The use of text messages through cell phones is unique to the 21st century. Never before have soldiers had the ability to receive messages from around the world at a moment's notice. While receiving updates from home is uplifting, receiving messages from the enemy can be a serious vulnerability.

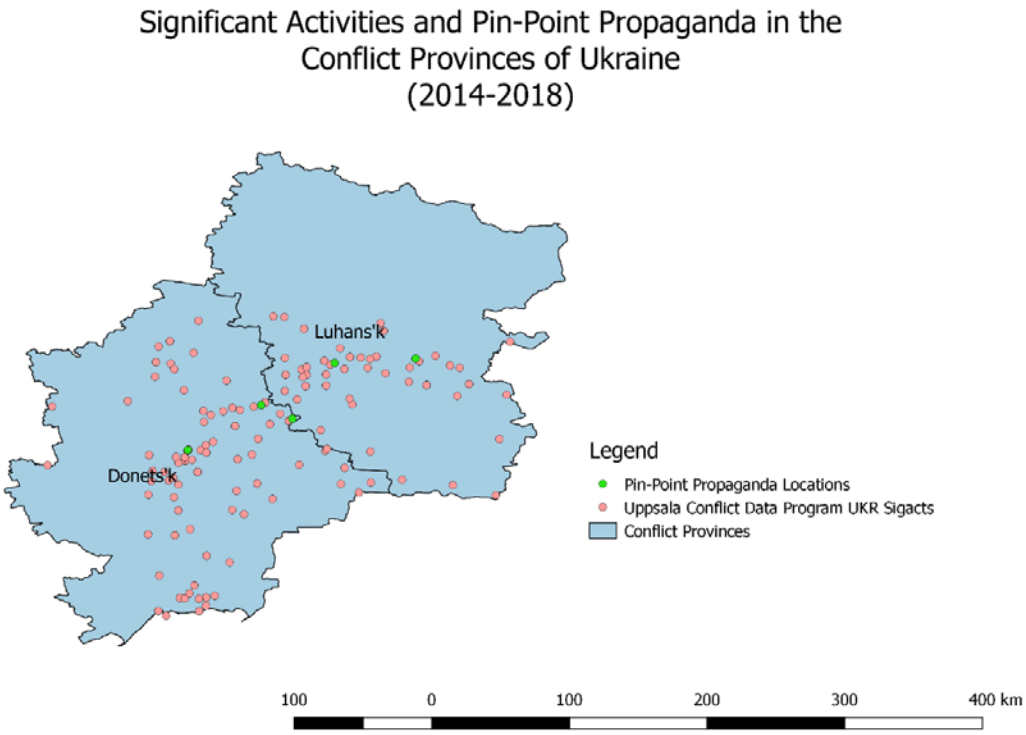



Figure 7. Map of Conflict Provinces with SIGACTs and Text Message Locations[87]

The Russians have taken traditional propaganda and modernized it to influence individuals or many individuals to have a profound impact on the battlefield. Figure 8 breaks down the topic of the propaganda text messages sent during the war in Ukraine. The topics consisted of the threat of imminent death, financial concerns, family heartstrings, becoming a puppet of the government, becoming a puppet of the military, false stories, civilian detriment, and retreat/surrender/go home. Of these messages, the most common dealt with imminent death and financial matters. The Russians were intentional when choosing who and what to target. The average Ukrainian soldier at the time was paid very little, under-equipped, and forced to live in austere conditions while deployed on "Antiterrorism Operations." Since one of the key effects of propaganda is to erode morale and cause desertions, these topics are especially successful for targeting a Ukrainian soldier.

87 Adapted from UCDP, "Ukraine"; Satter, "You're Just Meat."

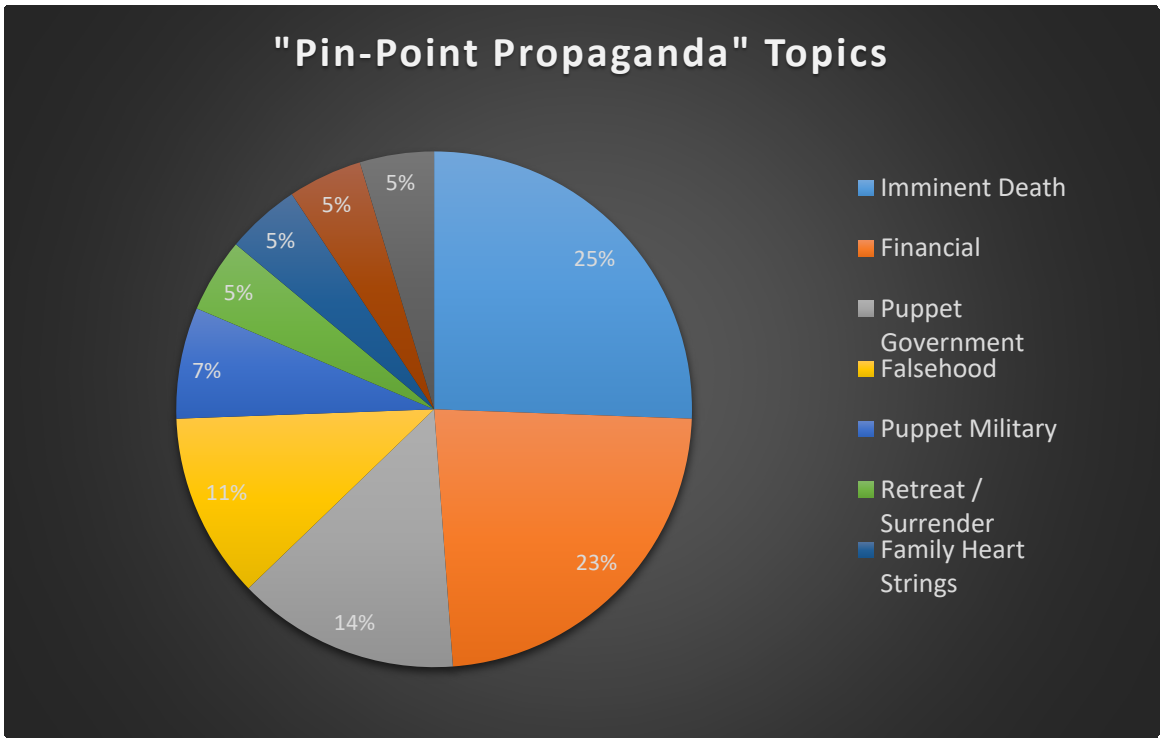



Figure 8. Propaganda Topics[88]

Of note, regular government troops from Ukraine were very susceptible to the effects of these targeted text messages, while members of the volunteer battalions were not; it only made them more upset and motivated them to attack Russian units.[89] The poor conditions facing government troops explains how inclined they were to be affected by the messaging. The years of corruption by government officials and contractors took a heavy toll on the Ukrainian military before the invasion even began.[90] The poor response of the military to the pro-Russian separatists showed the effects of low pay, poor training, and obsolete equipment. However, some volunteer forces were better-equipped thanks to the

88 Adapted from Raphael Satter, "IMSI Catchers in Ukraine," Google Docs, accessed May 11, 2020, https://docs.google.com/spreadsheets/d/1wnP1e-SS9_ArGX3M-miimJt-4SgmtSbUTraU10WMJKI/edit#gid=1560509081.

89 Aaron Brantly, "Defending the Borderlands of Europe: Ukrainian and American experience with IO, Cyber and EW," lecture, Defense Analysis Program, May 16, 2019, Naval Postgraduate School, Monterey, CA.

90 Kathy Lally, "Ukraine, Short on Military Budget, Starts Fundraising Drive," *Washington Post*, April 19, 2014, www.washingtonpost.com/world/europe/ukraine-short-on-military-budget-starts-fundraising-drive/2014/04/19/0eba04d0-c7f6-11e3-8b9a-8e0977a24aeb_story.html.

funding provided by wealthy oligarchs.[91] In many cases, the best members of the Ukrainian military joined the volunteer units for better pay and equipment. This made the volunteer units more effective and impaired the training of government units. These circumstances made the Ukrainian government troops more vulnerable to the directed propaganda from the Russians.

It is possible that significantly more messages were sent during this conflict. This is especially true when one considers the LEER-3 system "has a cell site simulator built into a drone that is capable of acting over a 6-kilometer-wide area and hijacking up to 2,000 cell phone connections at once."[92] Effectively, the LEER-3 system acts as a flying IMSI catcher, which gives the device a significantly larger range than a traditional ground-based system. With this coverage area, the LEER-3 may have affected many more people with Russian propaganda messages.

Figure 9 shows the number of text messages sent per year by location of where they were received. The cities of Avidiivka (2017), Schastia (2015), and Svitlodarsk (2016) all match up to battles that took place at these locations at the same time.[93] This coincides with the NGW Strategy of the Russians using text messages as a part of their IW capability to improve kinetic operations on the ground. While Debaltseve was not a battle site in 2015, it was a Ukrainian held position close to the front lines with Russian Separatists. Therefore, it was most likely the target of Russian IW and Psychological Operations as they attempted to influence the population and the Ukrainian security forces to withdraw.

[91] Deborah Sanders, "'The War We Want; The War That We Got': Military Reform and the Conflict in the East," *Journal of Slavic Military Studies* 30, no. 1 (2017): 42.

[92] Voice of America, "Sinister Text Messages."

[93] "Ukraine War Control Map & Report: June 2016," Political Geography Now, June 2016, https://www.polgeonow.com/2016/06/ukraine-war-control-map-report-june-2016.html.

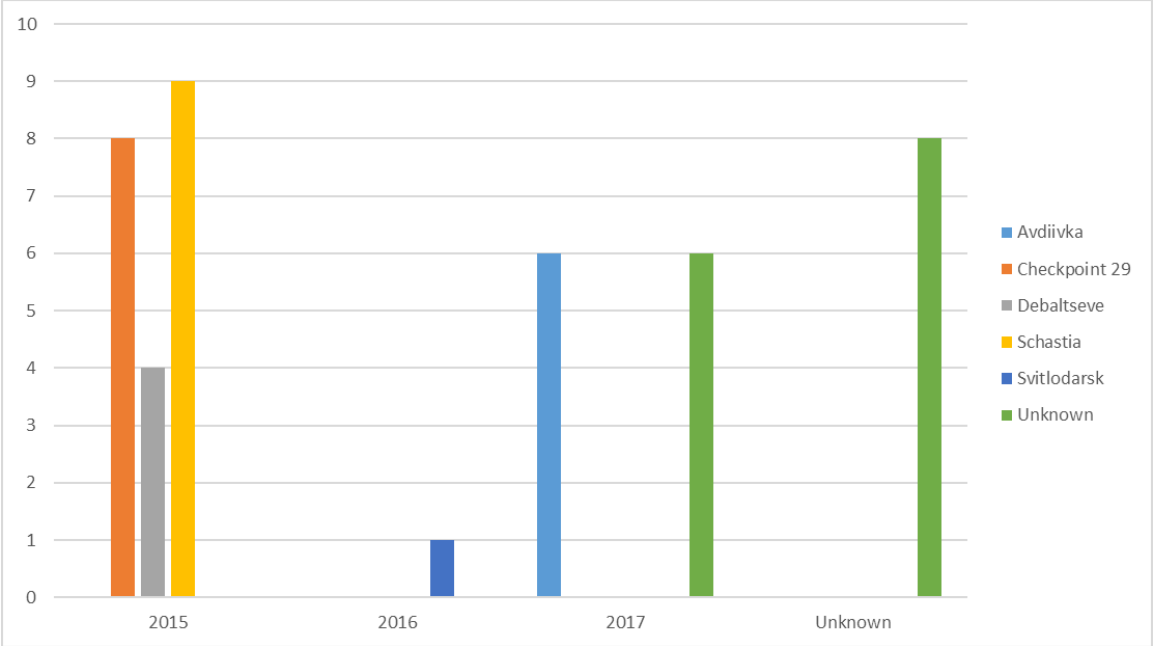



Figure 9. Texts per Year by Location[94]

The war in Ukraine has demonstrated the Russian ability to use messages from trusted communication sources, such as text (SMS), social media messaging, or email to target individuals on a mass scale. The consequence is the target is more likely to believe the message because it is from a trusted medium.[95] While the conflict in Ukraine has shown text messages to be effective tools for propaganda, they can also be used for more lethal means. The most extreme form of this phenomenon is described by Army Colonel Liam Collins, the Director of the Modern War Institute at West Point. He states:

> In one tactic, soldiers receive texts telling them they are "surrounded and abandoned." Minutes later, their families receive a text stating, "Your son is killed in action," which often prompts a call or text to the soldiers. Minutes later, soldiers receive another message telling them to "retreat and live," followed by an artillery strike to the location where a large group of cellphones was detected. Thus, in one coordinated action, electronic warfare

94 Adapted from Satter, "IMSI Catchers in Ukraine."

95 Giles, *The Next Phase of Russian Information Warfare*.

> is combined with cyberwarfare, information operations, and artillery strikes to produce psychological and kinetic effects.[96]

This example tragically illustrates the ability of the Russians to integrate fires and information warfare to achieve not just psychological effects but lethal effects as well. The vulnerability of cellular and smartphones is not limited to propaganda. Cellular and smartphones have deadly consequences that can affect units on the battlefield.

## D. AMERICAN EXAMPLE: FAKE DRAFT TEXT MESSAGE

Propaganda via cellular phone text message is not unique to Ukraine or the Russians. Americans have been hit by similar messages. Most recently, after the Iranian crisis in January of 2020, some American citizens reported receiving text messages on their phones about a mandatory military draft.[97] While the perpetrator of these messages is still unknown, as the case is currently under investigation, it does bring several interesting aspects to light.

The sender of these false military draft text messages smartly targeted a vulnerable American public. The timing was also effective as the messages were sent soon after the United States conducted an airstrike that killed Iranian Quds Force Commander, General Qasem Soleimani. This action increased the tensions between the two countries and caused speculations of war within various media camps. As a result, the American public was primed and more susceptible to believe and be concerned by a message about the military drafting civilians. Furthermore, the message used specific locations (cities and states) as well as the names of actual and fictional U.S. Army Recruiting Commanders to make them more believable.[98] The day after the airstrike took place, Google noted a surge in searches for "conscription," "Selective Service," and "Iran." The United States Selective Service

---

[96] Liam Collins, "Russia Gives Lessons in Electronic Warfare," Association of the United States Army, July 26, 2018, https://www.ausa.org/articles/russia-gives-lessons-electronic-warfare.

[97] Kim Bellware and Kayla Epstein, "Did You Get 'Drafted' by the U.S. Army via Text Message? It's a Hoax," *Washington Post*, January 8, 2020, www.washingtonpost.com/national-security/2020/01/08/army-draft-text-message-hoax/#comments-wrapper.

[98] "Army Recruiting Discredits Military Draft Texts," U.S. Army Recruiting Command, January 7, 2020, recruiting.army.mil/News/Article-Display/Article/2051787/urgent-news-army-recruiting-discredits-military-draft-texts/fbclid/IwAR22vIOsbx0KNcnZ-p0Igu0bIx2-GcBCjACJ2clbbLA9IPYBIEde_9_oduM/.

website also crashed as a massive influx of people went to the site looking for information. These text messages seek to weaken the trust citizens have in their government. They also build fear and paranoia within the citizenry. These feelings, when mixed with the right message, can bring internal unrest and fearmongering. The fake draft text messages show the vulnerability of people to the effects of phones being used as a vehicle of propaganda. It also illustrates that text message-based propaganda is not just limited to combatants or the battlefield; civilians and family members can also become targets.

## E. TARGETS OF CYBERSPACE EXPLOITATION

Not only can the public be seen as a vulnerable target, phones themselves can be the target of attacks on the battlefield, making the information environment as dangerous as any literal place on the battlefield. One of the key components of the information environment is the internet. Through the internet, one can share information and communications with millions of other users to spread ideas and information. It also has the potential to spread malware and other dangerous weapons that can take advantage of and harm users. Within the United States Department of Defense, cyberspace exploitations are "actions taken in cyberspace to gain intelligence, maneuver, collect information, or perform other enabling actions required to prepare for future military operations."[99] While many may consider the targets of cyberspace exploitation limited to computer systems, this section will demonstrate the vulnerability of cellular and smartphones to these actions.

Smartphones, which are very susceptible to malware and hacking, are within the purview of cyberspace exploitation. One reason for vulnerability is that "patches are not up-to-date because mobile devices are not scheduled for updates as frequently as desktop computers."[100] This allows nefarious actors to create exploits and malware that can easily infect and disrupt devices. Initially, Android devices were the only type targeted with malware. However, Apple iOS attacks are also becoming more common.[101] In Ukraine,

---

[99] Joint Chiefs of Staff, *Cyberspace Operations*, JP 3-12 (Washington, DC: Joint Chiefs of Staff), GL-4.

[100] Nick Ismail, "Common Security Vulnerabilities of Mobile Devices," *Information Age,* February 21, 2017, www.information-age.com/security-vulnerabilities-mobile-devices-123464616/.

[101] Ismail, "Common Security Vulnerabilities of Mobile Devices."

Android is the most popular phone type and was targeted by the Russians for the majority of their exploitations.[102] An excellent example of this is the hacking of a Ukrainian Fire Support Android Application.

The Ukrainian Army, at the time of the invasion, did not have enough fire control computers or encrypted communications equipment to allow for accurate and timely artillery fires. As a result, an officer of the 55th Artillery Brigade, Yaroslav Sherstuk, developed an Android operating system application to speed up the fire mission processing time for the D30 122mm towed howitzer.[103] The Russians were able to hack into this application and exploit it to gather the locations of the application's users and, as a result, the artillery unit itself. While the geolocation software on the phone was not enough to warrant an accurate target location, it was enough of an electronic signature to send other Intelligence, Surveillance, and Reconnaissance (ISR) assets to search the area. This often meant the Russians sent UAVs with sensors to better locate and target Ukrainian units. Once the target was found, the UAV would send the necessary location data to a Russian artillery system to strike Ukrainian emplacements and neutralize them. It is estimated that the Ukrainians lost 15% to 20% of all their D-30 artillery systems through the course of the war in the east.[104]

The Android application created by Sherstuk worked by streamlining and automating the requirements for artillery missions. Artillery needs five elements for accurate fire: accurate target location, location of the weapon to be employed, weapon data and ammunition characteristics, meteorological information, and finally, correct computations.[105] Sherstuk's artillery application made processing fire missions easy for

---

[102] Aaron Brantly, "Defending the Borderlands of Europe: Ukrainian and American Experience with IO, Cyber and EW," lecture, Defense Analysis Program, May 16, 2019, Naval Postgraduate School, Monterey, CA.

[103] "Use of Fancy Bear Android Malware in the Targeting of Ukrainian Field Artillery Units," CrowdStrike, December 22, 2016, https://www.crowdstrike.com/resources/reports/idc-vendor-profile-crowdstrike-2.

[104] CrowdStrike.

[105] Department of the Army, *Field Artillery Manual Cannon Gunnery*, TC 3-09.81 (Washington, DC: Department of the Army, April 2016), https://armypubs.army.mil/epubs/DR_pubs/DR_a/pdf/web/tc3_09x81.pdf.

artillery units. The user merely input the weather and target location. The application utilized the cellular phone's internal GPS to locate itself on the battlefield and, since it was designed for only the D30 howitzer, it had the necessary weapon and ammunition data already programmed within its coding. With this information, the application would automatically compute a firing solution which significantly decreased the time it took for artillery to receive, process, and then fire a mission. Where it used to take a firing element minutes to process a mission, Sherstuk's application computed a fire mission in under fifteen seconds.[106]

Eventually, Sherstuk's useful application found itself within the crosshairs of the Russians. Sherstuk never placed his application in the Android Market.[107] As a tactical tool, this is understandable as he did not want outside agents to get a hold of it or utilize its coding. This was also part of the application's undoing. Sherstuk advertised his application on a Ukrainian Military page which was posted to a Russian social media platform similar to Facebook, called VKontakte. He then attempted to control the dispersal of the application from his own website, as well as secure the application by issuing an activation code to screen users. By not placing the application on an authorized storefront, there was no way to control access to the application once it was in the open. Furthermore, Android, who at the time owned the Android Market where applications could be downloaded and bought, was unable to check the application to ensure it was free of malware.

As a result, the Russians were able to manipulate this legitimate application with a malicious attachment and allow it to spread.[108] The entity in Russia who is believed to have conducted this action is the cyber entity known as FANCY BEAR, who is thought to be part of the Russian Military Intelligence Agency, or the GRU. This is also the first time the GRU has been shown to manipulate Android operating software. To accomplish their attack, the GRU attached X-Agent malware to the application. X-Agent is a remote access

106 CrowdStrike, "Fancy Bear Android Malware."

107 CrowdStrike.

108 CrowdStrike.

toolkit that works against the operating systems of cellular phones.[109] This malware allowed the GRU to target users of the application and gain "access to contacts, Short Message Service (SMS) text messages, call logs, and internet data […] FANCY BEAR would likely leverage this information for its intelligence and planning value."[110] Effectively, the Russians used this malware to conduct cyber exploitation on the users' phones. With this information, the Russians could "map out a unit's composition and hierarchy, determine their plans, and even triangulate their approximate location."[111] The malware enabled the Russians to locate Ukrainian Artillery units which resulted in a clearer picture of the battlefield and the threat. This intelligence allowed the safer maneuver of separatist forces and the elimination of threat artillery systems.

In a similar case, several Ukrainian programmers were developing a secure military communications and navigation program called Network Bridge which became the target of Russian cyberspace exploitation.[112] This technology allowed Ukrainian soldiers to connect tablets holding gigabytes of topographical maps to tactical radios. The connection of these devices allowed soldiers to share tactical coordinates and messages securely throughout the battlefield. The programmers of this software team worked for a group called Army SOS. This entity continues to act as a fundraiser, donation collector, and technology support group to assist the Ukrainian Army.[113] By mid-2015, thousands of soldiers were using Network Bridge and the profile of Army SOS was growing. The programmers at Army SOS were soon targeted by the GRU—FANCY BEAR. On August 27, 2015, several dozen individuals who were contacts in one of the programmer's Gmail accounts received emails encouraging them to download the newest version of Network Bridge. However, the programmer never sent the email. It is believed the Russians were able to break into the programmer's email and send the message. The new version of

109 "X-Agent," New Jersey Cybersecurity and Communications Integration Cell, February 16, 2017, www.cyber.nj.gov/threat-profiles/trojan-variants/x-agent.

110 CrowdStrike, "Fancy Bear Android Malware."

111 CrowdStrike.

112 Raphael Satter, "Did CrowdStrike Really Miss the Mark?" Medium, July 20, 2018, medium.com/@rsatter/did-crowdstrike-really-miss-the-mark-ecedf0e09dd7.

113 "Army SOS," accessed February 3, 2020, armysos.com.ua/en/.

Network Bridge also had been modified with the "hidden ability to intercept messages and harvest GPS coordinates."[114] Fortunately, Gmail had flagged the infected emails. The Ukrainian programmers claimed the message was countered and the Russians' plans were foiled as none of the infected software was downloaded, according to the programmers. Nevertheless, this attack shows Russia's ability to infiltrate personal email accounts, manipulate applications, and deploy them through unassuming legitimate sources. It can be assumed the Russians used a similar stratagem in spreading a hacked version of the Ukrainian Fire Support Application.

The Russians, specifically the GRU, have a history of using inauspicious programs and modifying them with malicious code. The 2018 Winter Olympic Games were also a target of the Russian cyber operation called Olympic Destroyer. The Russians were banned from the games over illegal doping to give their athletes an unfair advantage.[115] In response, the Russians attacked the Winter Olympics being held in PyeongChang, South Korea. Olympic Destroyer cut off internet access, broadcast systems, the Olympics website, and ticket readers for many at the games during the opening ceremony.[116] The malware used in this attack was unique, as it included code from previously used malware attributed to the Chinese, North Koreans, and Russians.[117] The attack programs were deliberately manufactured to deceive those who would analyze it. Only after examining other components of the attack did it become apparent that Russia was the perpetrator.

One of the clues that led experts to believe Russia was the guilty party in the Olympic Destroyer attack was a nefarious Microsoft Word document that was sent to the staff at the Olympic committee two months before the games began. The Word file had "a

---

114 Satter, "Did CrowdStrike Really Miss the Mark?"

115 Karolos Grohmann, "Russia Banned from Pyeongchang Winter Olympics," Reuters, December 6, 2017, www.reuters.com/article/us-olympics-2018-russia/russia-banned-from-pyeongchang-winter-olympics-idUSKBN1DZ2QZ.

116 Ellen Nakashima, "Russian Spies Hacked the Olympics and Tried to Make it Look like North Korea Did it, U.S. Officials Say," *Washington Post*, February 24, 2018, www.washingtonpost.com/world/national-security/russian-spies-hacked-the-olympics-and-tried-to-make-it-look-like-north-korea-did-it-us-officials-say/2018/02/24/44b5468e-18f2-11e8-92c9-376b4fe57ff7_story.html.

117 Andy Greenberg, *Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers* (New York, NY: Random House, 2019), 256–57.

list of VIP delegates to the games but hid inside it a malicious macro script, the same simple program-in-a-document trick [… that the GRU had been] using in 2014." [118] By analyzing previous versions of similar tainted Word documents, the team of cybersecurity experts was able to locate a pattern of construction linking the Word document from the Olympic attack to previous Russian cyber-attacks.

By using fake applications for mobile devices, the Russians were able to insert Monokle malware into other unsuspecting targets. Monokle was designed for "stealing personal data stored on an infected device and exfiltrating this information to command and control infrastructure."[119] This particular piece of malware was created to target mobile devices using the Android operating system. The spread of the malware by hiding on targeted devices is what made these actions so effective. The Russians created fake applications like Skype, Signal and even Pornhub that looked and operated like the actual application but contained malware. These applications are commonly used by soldiers for communication and entertainment. A security intelligence engineer at the cyber security company Lookout stated, "This is a common technique that malware developers use. They 're-package' a well-known application with malicious functionality so as not to arouse user suspicion."[120] By hiding malware in common applications, the Russians have shown their ability to deceive end users.

Deception is an important component in cyber-attacks. As Gartzke and Lindsay put it, "Deception not only enables cyber attack, it is necessary: attackers who fail to be deceptive will find that the vulnerabilities on which they depend will readily be patched and access vectors will be closed."[121] Never before have so many gullible people been connected (through the internet) to something so vulnerable (computers and smartphones).

---

118 Greenberg, *Sandworrm*, 262.

119 Lookout, "Monokle: The Mobile Surveillance Tooling of the Special Technology Center" (research report, Lookout, July 2019), 3, https://www.lookout.com/documents/threat-reports/lookout-discovers-monokle-threat-report.pdf.

120 Patrick Tucker, "Russian Hackers Build Fake Skype, Signal, Pornhub Apps to Lure Victims," Defense One, July 25, 2019, www.defenseone.com/technology/2019/07/russian-hackers-build-fake-skye-signal-pornhub-apps-lure-victims/158713/.

121 Erik Gartzke and Jon R. Lindsay, "Weaving Tangled Webs: Offense, Defense, and Deception in Cyberspace," *Security Studies* 24 (2015): 326, 316–48, https://doi.org/1080/09636412.2015.1038188.

The access vectors open to cyber attackers are quite prolific. Malicious codes can be hidden in a variety of Microsoft Office tools (Word and PowerPoint) as well and PDF files, and even a recorded voicemail message. The GRU is successful in its cyber-attacks due to its ability to hide dangerous cyber tools in these innocent programs and files. The Russians had not only perfected the art of deception through computer programs, but also the exploitation of trusted sources.

In the case of the Ukrainian Artillery Android Application, the Russians knew "a military member would only trust and use an application designed to calculate something as critical as targeting data if it was developed and promoted by a member of their own forces."[122] The deception had to look like it came from a trusted source within the Ukrainian military for it be effective. Network Bridge shows a similar strategy. The Russians used the email of one of the software programmers to introduce the malware infected version of Network Bridge. Victims would be more inclined to believe a programmer involved in the creation of the software telling them to download a newer version. The Olympic Destroyer attack was built on multiple layers of deception as well. The malware was disguised as an innocent Microsoft Word document. The malware was composed of different pieces of code from North Korea, China, and Russia. The makeup of Olympic Destroyer not only deceives a user into activating its nefarious programming because it is disguised as a benign attachment, but once open it is hard to decipher who created the malware. Even Monokle depended on the user downloading a Trojanized application that seemed legitimate to deceive the user, but contained malware. These techniques exploit vulnerabilities of the user, and allows attackers to easily gain access to key decision-makers, facilities, and other critical components. If the user of the technology is not cautious and vigilant, they will fall prey to cyberspace exploitation regardless of platform. Cell phones offer the Russians just one more entry point from which to unleash their weapons.

The malicious modification of the Ukrainian Artillery Android Applications is but one example of a tool for cell phones being modified by a nefarious actor to exploit its

[122] CrowdStrike, "Fancy Bear Android Malware."

user. Fortunately, the developer of this application had a relatively small audience—artillery leaders. As a result, the effects of Russian cyberspace exploitation were kept at a fairly low level. Another more popular application may have had much deeper consequences. However, the psychological effect of this type of hacking should not be underappreciated. Ukrainian soldiers may now question all of their electronic equipment as being hacked by the Russians. A soldier may feel hesitant to use technology, as the repercussions of turning on the system could enhance their digital signature and make them a target for a kinetic attack. Ultimately, cyber operations have effects on both the cognitive and physical aspects of warfare.

## F. AMERICAN EXAMPLE: TIKTOK VIDEO APPLICATION

While all phones are susceptible to the effects of cyberspace exploitation, some of the most effective introduce these attacks through deception. The TikTok application represents one example of an effective cyberspace exploitation that is currently affecting the United States Department of Defense. According to its official website, "TikTok is the leading destination for short-form mobile video. Our mission is to inspire creativity and bring joy."[123] The application is immensely popular, with 1.4 billion downloads worldwide, and more than 120 million in the United States.[124] However, lawmakers in the United States believe the application has a more sinister purpose.

Members of Congress are concerned TikTok is censoring politically sensitive content (like the protests in Hong Kong). Furthermore, they are troubled with how TikTok stores the private data of its users and how China might use this information as a source of intelligence. United States Senator Marco Rubio stated in a tweet, "Any platform owned by a company in China which collects massive amounts of data on Americans is a potential serious threat to our country."[125] TikTok is not necessarily a platform for malware, but it

123 "TikTok," accessed May 3, 2020, www.tiktok.com/about?lang=en.

124 Drew Harwell and Tony Romm, "U.S. Government Investigating TikTok over National Security Concerns," *Washington Post*, November 1, 2019, www.washingtonpost.com/technology/2019/11/01/us-government-investigating-tiktok-over-national-security-concerns/.

125 Greg Roumeliotis, "Exclusive: U.S. Opens National Security Investigation into TikTok," Reuters, November 4, 2019, www.reuters.com/article/us-tiktok-cfius-exclusive/exclusive-u-s-opens-national-security-investigation-into-tiktok-sources-idUSKBN1XB4IL.

has the ability to collect information on its users and then share that data with its owners in a similar vein to what the X-agent malware does for the GRU. The Chinese may have perfected the use of deception in cyberspace exploitation. Instead of embedding malware to steal information in harmless files and programs, the Chinese have created an incredibly popular smartphone entertainment application to collect data and then used their own laws to allow the exploitation of that data and intelligence.

On 1 June 2017, the Chinese Government approved the Cyber Security Law of the People's Republic of China. These laws had some far-reaching and vague rules which all in China must obey. The laws "granted authorities the power to cut internet access in public security emergencies, and required data localization [sic] of servers in China as well as cyber security reviews of company data."[126] Furthermore, the law requires "internet company operators to cooperate with investigations involving criminal conduct and national security. Companies must give government investigators full access to their data if national security risks are suspected."[127] These laws allow the Chinese government access to the personal data of a country if it believes this data could assist in the national security of China. There was no clearly stated review process on what constitutes a "national security risk." This vague terminology could be used to divulge data from any company in China, including TikTok, who is owned by the Chinese company Beijing ByteDance Technology. As a Chinese-owned company, ByteDance must ensure that it follows these laws.

Due to the threat of its information collection for the Chinese government, the United States Department of Defense has banned TikTok on all government phones.[128] Many of the services have also encouraged its members to remove it from their personal phones. The United States Navy went a step further and stated that servicemembers with

[126] Max Parasol, "The Impact of China's 2016 Cyber Security Law on Foreign Technology Firms, and on China's Big Data and Smart City Dreams," *Computer Law & Security Review* 34, no. 1 (February 2019): 84, https://doi.org/10.1016/j.clsr.2017.05.022.

[127] Parasol, "The Impact of China's 2016 Cyber Security Law," 85.

[128] Ben Kesling and Georgia Wells, "U.S. Military Bans TikTok over Ties to China," Dow Jones Institutional News, January 3, 2020, http://libproxy.nps.edu/login?url=https://search.proquest.com/docview/2332264634?accountid=12702.

TikTok on their phones or tablets would be blocked from accessing the Navy Marine Corp intranet.[129] Recently, governments and citizens have voiced their concerns with privacy and big data collection from technology companies. The future of intelligence and cyberspace exploitation may lie in the creation of popular apps to collect data, which can then be analyzed and turned into intelligence, much like how cell phones can be exploited through malware today.

## G. OPERATIONAL SECURITY VULNERABILITIES

Cybersecurity experts state the weakest link in any computer or technology-related security system is the end-user. If the owner of the device is not willing to change the password or update virus protection, then they will be responsible for the exploitation of the device. The same can be said of phone users. Often the owner fails to read the fine print and obligations associated with the use of various applications and software. Negligence on behalf of the user in regard to a phone and its applications is also a problem, as well as, the posting of sensitive information and the unintentional use of applications to give away the location of different formations and bases. These actions are commonly referred to as OPSEC violations. OPSEC is defined as "A capability that identifies and controls critical information, indicators of friendly force actions attendant to military operations, and incorporates countermeasures to reduce the risk of an adversary exploiting vulnerabilities."[130] Nevertheless, what the United States military wants to limit are OPSEC Indicators, which are, "Friendly detectable actions and open-source information that can be interpreted or pieced together by an adversary to derive critical information."[131] In terms of smartphones and users, the biggest concern is the posting of open source information that has the potential to give away sensitive data by troops and civilians.

---

[129] Jeff Schogol, "The Pentagon Has Declared War on...*Checks Notes*... Tik Tok," Task & Purpose, December 19, 2019, taskandpurpose.com/news/dod-uninstall-tik-tok.

[130] Joint Chiefs of Staff. *Operational Security*, JP 3-13.3 (Washington, DC: Joint Chiefs of Staff, 2016), https://www.navy.mil/ah_online/OPSEC/docs/Policy/Joint_Publication_3-13.3_(6_Jan_2016)_Joint _OPSEC _Publication.pdf, GL-3.

[131] Operational Security, GL-3.

Failure to apply basic OPSEC considerations can reveal important information to the enemy and other nefarious actors. Perhaps the best example of this occurring in Ukraine is with a Russian serviceman named Bato Dambaev, who was a member of the 37th Motorized Infantry Brigade (Kyakhta).[132] During the initial stages of the conflict in Ukraine, the Russian government refused to acknowledge the presence of its military forces within the borders of Ukraine. On 16 April 2015, Vladimir Putin, President of the Russian Federation, stated on his popular call-in show, "Direct Line with Vladimir Putin," that, "I can tell you outright and unequivocally that there are no Russian troops in Ukraine."[133] However, evidence of Russian involvement was found throughout Ukraine, as illustrated by the bodies of dead Russian citizens, Russian weapons, and in photos throughout the internet.[134]

VICE News and the investigative service Bell¿ngcat (referred throughout this thesis as Bellingcat) which is, "an independent international collective of researchers, investigators and citizen journalists using open source and social media investigation to probe a variety of subjects," tracked the movement of Bato and his unit into Ukraine.[135] Together these two entities created the documentary, *Selfie Soldiers: Russia Checks into Ukraine*. The documentary used geotagged photos posted by Bato on his VKontakte (VK), the Russian equivalent of Facebook, social media page. Bato's photos documented his train up at various military facilities in Russia and his eventual deployment in Ukraine. The reporters retraced his steps by using photos from his VK account. Once they had found the correct location, the reporters would then recreate selfies at the same locations where Bato had initially taken the photos (see Figure 10).

---

132 Aric Toler, "Russia's 'Anti-Selfie Soldier Law': Greatest Hits and Implications," Bellingcat, February 21, 2019, https://www.bellingcat.com/news/uk-and-europe/2019/02/20/russias-anti-selfie-soldier-law-greatest-hits-and-implications/.

133 "Direct Line with Vladimir Putin," Kremlin, April 16, 2015, http://en.kremlin.ru/events/president/news/49261.

134 Simon Ostrovsky, "Russia Denies That its Soldiers Are in Ukraine, But We Tracked One There Using His Selfies," Vice, June 16, 2015, www.vice.com/en_us/article/ev9dbz/russia-denies-that-its-soldiers-are-in-ukraine-but-we-tracked-one-there-using-his-selfies.

135 "About," Bellingcat, accessed May 8, 2020, https://www.bellingcat.com/about/.

By comparing Bato's photos with the reenacted selfies, side by side, the documentary team proved that the Russian government had deployed troops within the legal borders of Ukraine.[136] These actions showed the vulnerability of an unsuspecting end-user to give away crucial military information. The ignorance displayed by many people in terms of their digital footprint and the information they post to social media can cause a great deal of damage and can even have strategic implications.

Journalist Simon Ostrovsky (right) re-creating one of Bato Dambaev's personal photos from his deployment in Ukraine.

Figure 10. Re-creation of Russian "Selfie" in Ukraine[137]

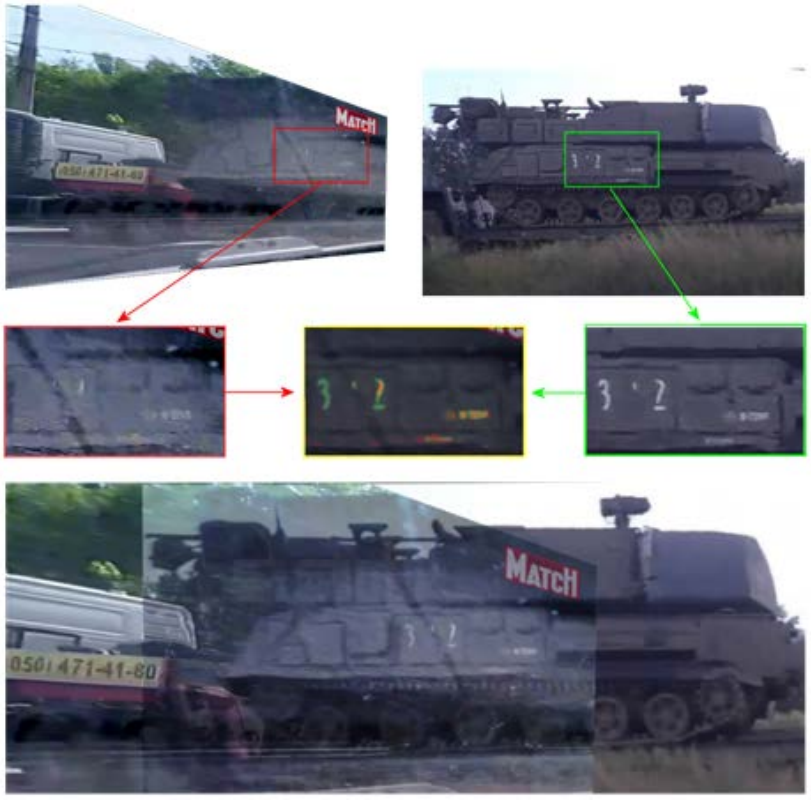
Furthermore, the team at Bellingcat was also instrumental in determining the truth about what happened to Malaysian Airlines Flight 17 (MH17). A Malaysian Airways Boeing 777, civilian airliner crashed into the conflict region of Eastern Ukraine on 17 July 2014.[138] The aircraft carried 298 people whom all perished in the crash. The incident sparked fierce accusations among nations in the region and those who had citizens on board

136 Toler, "Russia's 'Anti-Selfie Soldier Law.'"

137 Source: Ostrovsky, "Russia Denies That its Soldiers Are in Ukraine."

138 "MH17 Ukraine Plane Crash: What We Know," BBC, February 26, 2020, www.bbc.com/news/world-europe-28357880.

the flight.[139] These accusations initiated a major investigation into what caused the downing of the airliner. The evidence, in this case, included things outside the scope of typical aircraft crashes. While the physical debris would give important clues, other vital pieces of information were to be found within the information environment.




The above image shows how a photograph (red frame) can be compared to a different photo (green frame) by using a flattening process to compare two images (yellow frame).

Figure 11. Imagery Comparison of the Russian Buk Air Defense Missile Launcher[140]

Bellingcat, using OSINT, again mostly from social media, was able to determine not just what country was responsible for the downing of the aircraft but what unit and which launcher was utilized in the illegal attack. In the aftermath of the MH17 crash, there was a large amount of activity on social media as well as photos and videos on the accused

139 "Malaysia Airlines MH17 Crash: What We Know So Far," *Guardian*, July 18, 2014, www.theguardian.com/world/2014/jul/18/mh17-crash-what-we-know-so-far-malaysia-airlines-ukraine.

140 Source: "Origin of the Separatists' Buk: A Bellingcat Investigation," Bellingcat, November 18, 2014, www.bellingcat.com/news/uk-and-europe/2014/11/08/origin-of-the-separatists-buk-a-bellingcat-investigation/.

Buk missile system being transported through the area.[141] Using a collection of photos from different sources and different image manipulation software, as well as geolocation techniques, and embedded photo timestamps, Bellingcat recreated the route the launcher took into eastern Ukraine and determined its presence on 17 July 2014. On the date of the aircraft crash, the launcher was located in an area where it would have been able to engage MH17. On 18 July, the same launcher was photographed leaving the area with one of its missiles missing. The main give away of the vehicle was its number (see Figure 11). In many militaries throughout the world, each vehicle has what is referred to as a bumper number. This number allows each unique vehicle to be identified despite being the same general type of vehicle. With the bumper number and other unique features of the offending launcher, Bellingcat could track the vehicles as it moved through eastern Ukraine and eventually back to its base in Kursk, Russia.

Furthermore, Bellingcat was able to identify the unit and then built up its chain of command through social media posts made by its members. To determine who on social media was a part of the unit, the "Bellingcat team used photos of badges, patches, emblems, other symbols visible on the soldiers' uniforms as well as flags and other distinguishing objects in order to determine in which unit a soldier was or is currently serving."[142] From this information, it became evident that the unit responsible for the attack was the 53rd Anti-Aircraft Missile Brigade. These unique objects proved critical in differentiating what unit troops were assigned. Also interesting is Bellingcat's discovery of an online forum used by the mothers, wives, and girlfriends of the soldiers in the 53rd Brigade.[143] Their posts revealed the names of several members of the unit and gave details about where the unit was going and the activities they conducted. The names of these soldiers helped the investigators to find their social media profiles, which unearthed more names and more members of the Brigade. When examining the social media profiles of the different soldiers, Bellingcat would also look at their mutual friends and look for other connections

141 Bellingcat, "Origin of the Separatists' Buk."

142 Daniel Romein, *MH17—Potential Suspects and Witnesses from the 53rd Anti-Aircraft Missile Brigade: A Bellingcat Investigation* (Bellingcat, 2016), 7.

143 Romein, *MH17*, 36.

to see who else would be a part of the 53rd Brigade. Eventually, Bellingcat was able to recreate the 53rds chain of command (see Figure 12). Their investigative work was given to the Joint Investigative Team lead by the Dutch and is being used by the prosecution in their current court case over who is culpable in the downing of flight MH17.

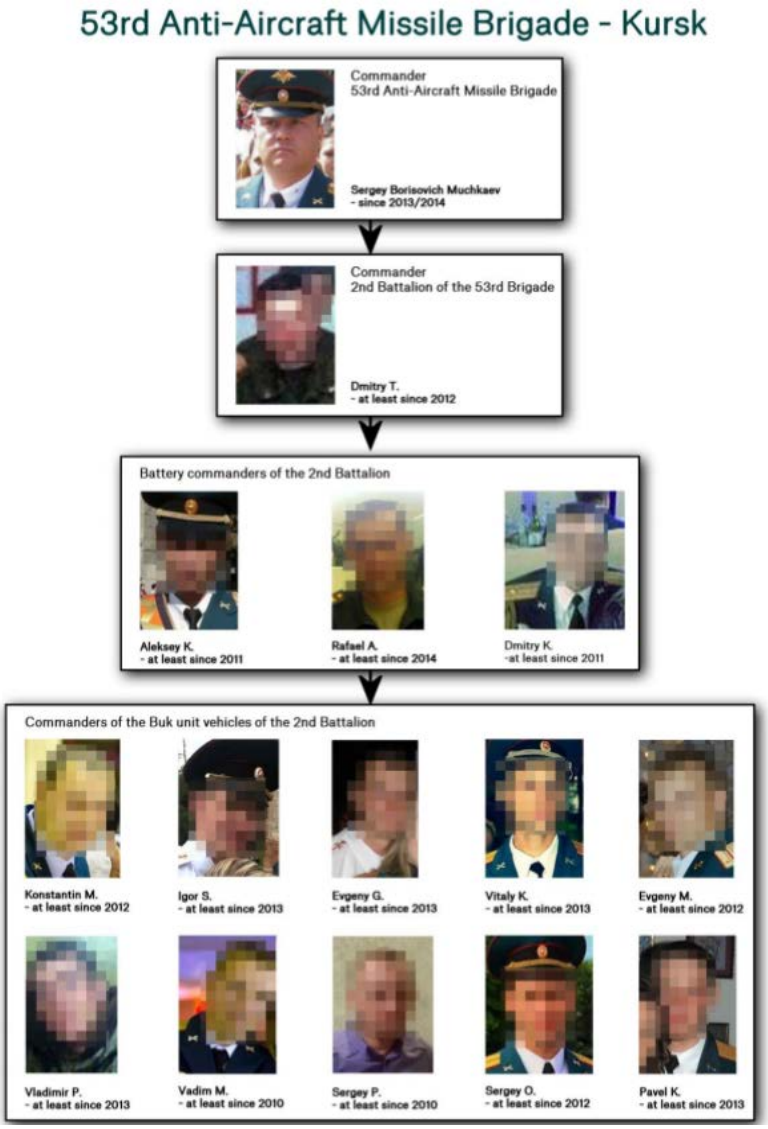



Figure 12. The 53rd Anti-Aircraft Missile Brigade Chain of Command as Discovered by Bellingcat[144]

144 Source: Romein, 110.

The MH17 incident and the work done by Bellingcat show several vectors for OPSEC exploitation. Even though posts to social media and the tagging of photos is fairly obvious, more interesting is the exploitation of military forums for spouses, relatives, and friends. These can be treasure-troves of information. The users of these forums often have little to no OPSEC training and could give away some extremely valuable information. It is a common practice among military members to change their names on social media platforms. However, Bellingcat has shown that by comparing mutual friends through different social media platforms that the true identity of a user can be found relatively easily.

## H. AMERICAN EXAMPLE: STRAVA FITNESS APPLICATION

The United States is not immune to these violations of operational security. Recently, some classified facilities in the United States Central Command region were exposed by personnel using fitness applications on their smartwatches. Strava is a fitness networking application that "turns every iPhone and Android into a sophisticated running and cycling computer (and we work with your GPS watches and head units, too). Start Strava before an activity and you can track your favorite performance stats, and afterwards, dive deep into your data."[145] Many of these devices use the internal geolocation software of a user's phone or fitness tracking device to measure the distance and speed of a user's workout. These devices are then linked through a social media-like platform to a network of other users to display statistics and locations. The Strava application allows the user to comment, share, attach photos, and look at popular workout locations. This is troublesome when one is looking at OPSEC concerns. Many of these features, which are enjoyable in the civilian world, can have disastrous consequences on the battlefield.

One feature of Strava is its "Heatmap," which examines geographic location by the amount of exercise activity that occurs within it. Strava states "The heatmap shows 'heat' made by aggregated, public activities over the last two years."[146] When examining the heat

145 "Features," Strava, accessed May 8, 2020, www.strava.com/features.

146 "The Global Heatmap," Strava, accessed May 8, 2020, www.strava.com/heatmap#8.69/44.72259/33.44340/hot/all.

map, one can see vastly illuminated areas within Europe, the United States, Brazil, and other developed areas of the world. When one examines conflict zones, the map is dark due to a lack of tracked activity. However, if these areas are zoomed in, one would find small pockets of activity. Service members on small remote bases used Strava to record their workouts and inadvertently gave away the location of their secretive facilities.

An Australian University student was the first to publish these findings after discovering them in November of 2017.[147] Nathan Ruser stated that he got the idea after his father mentioned the Heatmap showed "where rich white people are" located on earth. From that, he began to wonder if the map could be used to find U.S. military personnel. Once Ruser posted his observations to Twitter, others began to look for and find secret U.S. bases. Even more troubling is that the device also tracked patrol routes of U.S. troops. Since many people are concerned with step counts and tracking distances, many soldiers would leave the devices on during patrols in combat areas. The activity was recorded and then added to the Heatmap.

Strava unintentionally collected what intelligence analysts call a pattern of life. From the Heatmap, one could locate isolated secret bases, track the perimeter of the bases, find where soldiers conducted physical fitness, and observe patrol routes. All of these datapoints could be used by nefarious forces to target U.S. bases and units while they were out on a mission.

## I. CONCLUSION

Through much of the 20th century, soldiers were told not to smoke at night as the glowing embers could give away their position. For years, the military stressed "light and noise discipline" when in a field environment. This meant when on patrol, soldiers could not smoke or talk freely for fear the enemy would notice their presence. In today's modern battlefield, a smartphone and some careless posts on social media may have a similar effect for a smart adversary. The tactical consequences of Bluetooth technology (or any other

147 Liz Sly, "U.S. Soldiers Are Revealing Sensitive and Dangerous Information by Jogging," *Washington Post*, January 29, 2018, www.washingtonpost.com/world/a-map-showing-the-users-of-fitness-devices-lets-the-world-see-where-us-soldiers-are-and-what-they-are-doing/2018/01/28/86915662-0441-11e8-aa61-f3391373867e_story.html.

electronic signature from a smartphone) might be similar to those of cigarettes in 21st-century combat. Small unit leaders must enforce strict control over the use of cellular and smartphones by their subordinates. Armed with the knowledge of the repercussions from the careless use of personal electronic devices, troops should be more apt to curtail the use of their devices in the tactical arena.

The examples from the Russian Invasion of Ukraine in 2014 show the vulnerability of cellular and smartphones to troops on the battlefield. The use of flying IMSI Catchers to send targeted propaganda messages to the personal phones of soldiers is a challenge American forces have never faced. The hacking of useful mobile device applications, like the Ukrainian Artillery Android Application, to expose the user location or other information is another challenge American military personnel have not had to contend with in battle. Finally, while military leaders understand the risk of OPSEC, its effects are not clearly articulated to lower-level troops. This is illustrated clearly in the social media posts of Bato Dambaev and the Russian 53rd Anti-Aircraft Missile Brigade as they operated in Ukraine despite President Putin saying otherwise causing international uproar and creating strategic problems for the Russian government to face. With an understanding of current vulnerabilities, the United States needs to look at future threats from cellular and smartphones in order to form effective solutions to this dire problem.

# IV. THE FUTURE THREAT OF CELLULAR AND SMARTPHONES

While the current vulnerabilities from the use of cellular phones have proven to be dangerous and troublesome, the future may become even more perilous. New technologies currently exist that are on the brink of changing the way people retrieve and use information. The development of 5G networks and the creation of the IoT have the promise of making life better. However, the emergence of 5G network exploits, deepfake video, and other technologies will also shift how mobile devices can be manipulated. This chapter will examine the future vulnerabilities of cellular and smartphones to military organizations. The chapter will examine each future vulnerability by using the same framework of threats used in the Ukrainian case study of propaganda, offensive cyberspace operations, and OPSEC concerns. By examining the risk of future cellphone use in the military through these three vulnerabilities, one can gain a better understanding of how future technology may affect troops on the battlefield

## A. PROPAGANDA

Actions in Ukraine have presented new vectors for propaganda. While electronic messaging is nothing new, the ability to effectively target specific segments of a group, or certain individuals, is a recent advancement in propaganda. Tailoring messages to specific individuals will ensure that propaganda continues to evolve and become more effective. Libicki, in 1995, envisioned improvements to psychological operations by "telling soldiers that their wives are sleeping around [ … which would be] more effective if those at home can be identified by name. [… This] would be easier in advanced societies, which these days generate enormous computer-kept files on almost everyone."[148] The use of specific names to precisely target propaganda will make it significantly more effective. The "enormous computer kept files" that Libicki speaks of exist in the United States in the form of the Office of Personnel Management (OPM). Unfortunately for many members of the United States military, the Chinese government already has this data.

148 Libicki, *What Is Information Warfare*, 40–41.

The stealing of valuable information from the Office of Personnel Management, commonly referred to as the OPM hack, may prove to have been one of the most effective cyberspace exploitations against the United States. In 2014, the Chinese successfully conducted two cyberspace exploitations on "U.S. government databases holding personnel records and security-clearance files which exposed sensitive information about at least 22.1 million people, including not only federal employees and contractors but their families and friends."[149] One of the most important pieces of data collected by the Chinese was the Standard Form 86 or SF86, which is a questionnaire every person applying for a security clearance must complete. This includes government workers, military personnel, and contractors. The SF86 is used to gather information for security investigators to ensure the applicant is not a threat and can be trusted with classified information. The data on this form includes the contact information and personally identifiable information of close family members, trusted friends, and colleagues. Thus, the OPM collected a completed SF86 for every person who applied for a security clearance in the United States. The Chinese now have the contact information of all these personnel and some of their most trusted associates. With this treasure trove of information, the Chinese have achieved the capability that Libicki postulated about twenty-five years ago and ensured their intelligence apparatus could target U.S. military personnel and their families with propaganda and threats.

These messages could have significant effects on the battlefield and in military operations. Imagine a U.S. Naval vessel conducting freedom of navigation operations along the Spratly Islands in the South China Sea. Then imagine the ranking naval officer receiving an ultimatum via his phone or other device threatening the life of his family if he does not leave the area and cease his 'infringement' into Chinese territory. What if a number of the enlisted crew received these messages? The result could be widespread panic or a possible mutiny. Messages like this could be used to prevent U.S. military incursions

[149] Ellen Nakashima, "Hacks of OPM Databases Compromised 22.1 Million People, Federal Authorities Say," *Washington Post*, July 10, 2015, www.washingtonpost.com/news/federal-eye/wp/2015/07/09/hack-of-security-clearance-system-affected-21-5-million-people-federal-authorities-say/.

and influence in contested areas. It could also be used to prevent the military from conducting joint training with partner forces.

In addition to risking the success of military operations, targeted messages could also be used in the diplomatic and intelligence realm. With the OPM information, it would be easy for China or other countries to locate and exploit intelligence personnel located in nearby U.S. embassies. With the contact information of the close relatives of every person who has a clearance, attackers could piece together who works at the different embassies and then target them and their families. The messages may vary from physical threats to 'False Flag operations,' which are attempts to recruit intelligence operatives to join what they are being told is a U.S. Operation that is actually being run by another nation.

While the loss of intelligence assets and diplomatic officials is alarming, the unknown actor who possesses this data represents the real danger. The information gained from the OPM hack may have been shared with other countries and even some non-state actors. This valuable data has the ability to threaten the United States with detailed information necessary for counterforce psychological operations on U.S. personnel at many different levels within the government.

Deepfake videos that manipulate audio and visual information are another possible type of propaganda. The term deep fake comes from the combination of "deep learning," a subset of machine learning, and "fake news."[150] The use of deception to get people to do things they normally would never do is not a new idea. However, technology has now reached a point where video images can be manipulated to deceive a viewer into believing something that is not true.[151] The comedian and writer Jordan Peele demonstrated this by taking a video of former President Barack Obama and modifying it so as to make him say things he would never say in real life.[152] The video also highlights the dangers of deep

[150] Joe Littell, "Don't Believe Your Eyes (or Ears): The Weaponization of Artificial Intelligence, Machine Learning, and Deepfakes," War on the Rocks, October 7, 2019, warontherocks.com/2019/10/dont-believe-your-eyes-or-ears-the-weaponization-of-artificial-intelligence-machine-learning-and-deepfakes/.

[151] Tom Van de Weghe, "Six Lessons from My Deepfake Research at Stanford," Medium, June 7, 2019, medium.com/jsk-class-of-2019/six-lessons-from-my-deepfake-research-at-stanford-1666594a8e50.

[152] Jordan Peele's video can be viewed on YouTube at https://www.youtube.com/watch?v=cQ54GDm1eL0.

fakes and the need to be critical of the information one consumes and shares. The imagery of Jordan Peele's video was seamless, and it appeared as if it was actual footage of President Obama saying outlandish things. Mobile streaming and video services continue to become more popular and the consumption of this video is staggering. Nearly "500 hours of video are uploaded to YouTube every minute [… and people] watch over 1 billion hours of YouTube videos a day, more than Netflix and Facebook video combined."[153] Mobile devices, including phones and tablets, represent 70% of YouTube's total views.[154] With these statistics, one can see how online videos can be used to reach large audiences in a short period of time.

The use of video to propagate deepfakes through vast segments of the population allows targeted propaganda to infect the battlefield and civilians on the home front. Alternately, at the strategic level, the United States could fabricate a deepfake video of an enemy national leader stating, "The war is over and the military needs to surrender," this could be an effective way of dissolving enemy military resistance and decreasing support for the war within the enemy populous. At a more tactical level, deepfake videos could be created and spread of individual unit commanders giving similar surrender messages to troops to degrade the fighting power of smaller units. These videos have the potential to lower the number of enemy forces the United States would have to fight due to desertion and surrender. In a more sinister capacity, the deepfakes might be used to degrade an ally with the United States.[155] False video of world leaders insulting partner countries could be used to erode support for coalitions or alliances. Deepfakes could segment populations along traditional rifts (race, sex, income, or social level) in order to decrease support for governments or to shift focus to internal issues and allow another country the freedom to act as it pleases on the international stage.

---

153 "57 Fascinating and Incredible YouTube Statistics," Brandwatch, February 21, 2020, www.brandwatch.com/blog/youtube-stats/.

154 Brandwatch.com., "57 Fascinating and Incredible YouTube Statistics."

155 Robert Chesney and Danielle K Citron, "Disinformation on Steroids: The Threat of Deep Fakes," Council on Foreign Relations, October 16, 2018, www.cfr.org/report/deep-fake-disinformation-steroids.

By mixing deepfake video technology and information from the OPM hack, combined with effective influence techniques used by the Russians in the 2016 election, it becomes nearly impossible to separate fact from fiction. The use of phones and other devices to spread these false video messages and propaganda only makes matters worse. Russia's actions in Ukraine have shown the threats posed to soldiers at the tactical level. As these actions are studied and improved with new technology, the effects of these deception operations can easily be upgraded to the national and strategic level.[156]

## B. CYBERSPACE EXPLOITATION

The ability to conduct cyberspace attack and cyberspace exploitation will increase in importance for nations and non-state actors as the world continues to connect itself through the internet and other modernized networks. The development and implementation of 5th Generation mobile networks and the rise of the IoT will create new vectors for attackers to execute their operations. The growth of the internet and the development of new networks may close some older access points for cyberspace attacks, but it will surely open new vulnerabilities for exploitation.

Future attack methods have already been developed by university students and researchers to utilize exploits in 5G technology. The Tracking via Paging mEssage DistributiOn (TORPEDO) attack utilizes an exploit in 4G and the current version of 5G through the use of "paging."[157] When a mobile device receives a call or text message, it needs an alert to move it out of its energy-saving mode. This process is called "paging." When there are multiple pages, "the network's Mobile Management Entry (MME) asks base station(s) to broadcast a paging message, which includes the Temporary Mobile Subscriber Identity (TMSI) of the device. The TMSI is assigned by the MME [… and should change] frequently."[158] Unfortunately, the TMSI, in practice, is rarely changed for each phone. As a result, an attacker can call a phone multiple times and, while looking at

156 Littell, "Don't Believe Your Eyes (or Ears)."

157 Syed Hussain et al., "Privacy Attacks to the 4G and 5G Cellular Paging Protocols Using Side Channel Information," NDSS Symposium (2019): 1, https://www.ndss-symposium.org/ndss-paper/privacy-attacks-to-the-4g-and-5g-cellular-paging-protocols-using-side-channel-information/.

158 Hussain et al., "Privacy Attacks," 1.

the paging messages, find the most frequent TMSI to conclude the victim is present in a given area. Text messages can also be used as a catalyst to send pages to the victim's device. With this information, an attacker can locate a user from their TMSI. To be successful, an attacker needs a pattern of life for their victim. Once the attacker knows the "victim's often-visited locations, then the attacker can set up sniffers on those locations to create the victim's cell-level mobility profile."[159] This information allows an attacker to know when a victim is in the area and if their device is operating. Attackers can "hijack the paging channel, enabling them to send fabricated emergency messages, mount a denial-of-service attack by injecting fabricated, empty paging messages, and thus blocking the victim from receiving any [calls or text messages]."[160] Many people believe that with the latest 5G technology that their devices will be safe, but TORPEDO shows that any device is capable of exploitation.

TORPEDO attacks can act as the precursor to other types of cyberspace exploitations on current 4G and future 5G phones such as Persistent Information ExposuRe by the CorE network (PIERCER).[161] The attacker uses TORPEDO to find the victim and ensure their mobile device is activated. Following the TORPEDO attack, the aggressor can then use the PIERCER to obtain the victim's IMSI on 4G networks. Some communications companies use IMSIs instead of the TMSI for their pages. By conducting some tests, researchers "revealed that it is possible to give the service provider the impression that the exceptional case [the use of IMSI instead of the approved TMSI for paging] is occurring which forces it to reveal the victim's IMSI."[162] PIERCER uses the inherent vulnerability of using IMSIs during paging to allow attackers to obtain a user's IMSI. Acquiring the IMSI allows older previously discovered attacks to be executed on the 4G platform.

In the case of a more secure 5G network and a service provider that practices proper protocol by using TMSI for paging instead of the more vulnerable IMSI, an attacker can

---

159 Hussain et al., 2.

160 Mohit Kumar, "New Attacks against 4G, 5G Mobile Networks Re-Enable IMSI Catchers," Hacker News, February 25, 2019, thehackernews.com/2019/02/location-tracking-imsi-catchers.html.

161 Hussain et al., "Privacy Attacks," 2.

162 Hussain et al., 2.

use IMSI Cracking to obtain the victim's IMSI. Following a successful TORPEDO attack, where the service provider uses TMSIs, the aggressor can utilize IMSI Cracking which conducts a brute-force attack on the victim's device to obtain their IMSI.[163] With the IMSI acquired, attackers can use conventional IMSI Catchers eavesdrop on victims' calls and discover their location "even if the victim owns a brand new 5G handset."[164] However, these attacks have their limitations and can take a long time to execute—IMSI Cracking can take up to thirteen hours.[165]

The vulnerabilities exploited by Russia in the 2G environment of Ukraine in 2014 can, unfortunately, be replicated with new cyber weapons such as TORPEDO and IMSI Cracking in the modern 5G environment.[166] The creation of these cyber weapons shows the vulnerability of any mobile device and network. It can be assured that motivated hackers will continue to refine these attacks and their necessary equipment to make them more efficient for more elaborate operations.

Embassies and diplomatic missions throughout the world have been used as projection points for espionage and they may also soon be jumping-off points for cyberspace exploitation. Using modern attack methods and IMSI Catchers, it is possible that a country could collect mobile device information and broadcast messages as shown by illegal cellular stations in China and Russian drones in Ukraine. Such actions have already been uncovered in Washington, DC, by the Israelis. Politico reported that Stingray devices "formally called international mobile subscriber identity-catchers or IMSI-catchers, […] capture the contents of calls and data use. The devices were likely intended to spy on President Donald Trump, one of the former officials said, as well as his top aides

163 Gareth Corfield, "Latest 4G, 5G Phone-Location Slurp Attack Is a Doozy, but Won't Torpedo Average Joe or Jane," The Register, February 26, 2019, www.theregister.co.uk/2019/02/26/torpedo_piercer_attacks/.

164 Kumar, "New Attacks against 4G."

165 Hussain et al., "Privacy Attacks," 2.

166 Bozhena Shermeta, "Stuck in 2G, Moving to 3G as Other Nations Zoom to 4G," *Kyiv Post*, May 29, 2015, kyivpost.com/article/content/doing-business-in-ukraine/stuck-in-2g-moving-to-3g-as-other-nations-zoom-to-4g-390959.html.

and closest associates."[167] Intelligence organizations will always seek ways to exploit the newest forms of technology.

The spread of 5G technology has been controversial for the United States and its allies. The Chinese through Huawei have become one of the leaders in propagating 5G technology throughout the world.[168] The United States remains skeptical of the security of current 5G networks developed by Huawei. Leaders in the United States are wary of the information that moves through the Hauwai 5G network can be collected and then acted upon by the Chinese government.[169] While the thought of another great power using 5G to collect intelligence is unsettling, the reason for its creation, the IoT, may have greater vulnerabilities than the network itself.

The IoT is facilitated by the development of faster 5G Network Technology. As more objects are connected to the internet, more attack vectors are opened to hackers around the world. Robert Spalding stated, "5G is not just for refrigerators. It's farm implements, it's airplanes, it's all kinds of different things that can actually kill people or that allow someone to reach into the network and direct those things to do what they want them to do. It's a completely different threat that we've never experienced before."[170] Just like the sudden introduction and consumption of mobile devices, one can expect similar results with new devices and the IoT. However, with this sudden influx of new technology comes a sizable lag in the introduction of effective patches and virus detection software.[171] Furthermore, each of these new devices that are created for the IoT has unique characteristics and programming which make it difficult for a universal type of virus

---

[167] Daniel Lippman, "Israel Accused of Planting Mysterious Spy Devices near the White House," *POLITICO*, September 12, 2019, www.politico.com/story/2019/09/12/israel-white-house-spying-devices-1491351.

[168] Brian Fung, "How China's Huawei Took the Lead over U.S. Companies in 5G Technology," *Washington Post*, April 10, 2019, www.washingtonpost.com/technology/2019/04/10/us-spat-with-huawei-explained/.

[169] Sue Halpern, "The Terrifying Potential of 5G Technology," *New Yorker*, April 30, 2019, www.newyorker.com/news/annals-of-communications/the-terrifying-potential-of-the-5g-network.

[170] Halpern, "Terrifying Potential."

[171] Lily Hay Newman, "An Elaborate Hack Shows How Much Damage IoT Bugs Can Do," *Wired*, December 10, 2018, www.wired.com/story/elaborate-hack-shows-damage-iot-bugs-can-do/.

detection system. Currently, some of the most common platforms used to gain entry for hackers include: wireless cameras, baby monitors, smart thermostats, and smart door locks (Ring systems).[172] It is only a matter of time before devices like Amazon's Alexa and Google Home's smart speakers are also exploited.

An attack on the IoT may prove to be easier than contemporary cyber-attacks. M. Carlton, the vice president of research at Senrio, a network security company, stated that attacks through the IoT show "why it's important to know what's really on your network. These devices are all connected to each other and can create a hole in the network. It would be very difficult to catch this."[173] Instead of hobbling together malware code from various sources, a hacker may be able to bypass the deception means by exploiting easy attack vectors inside the everyday objects and appliances that are connected to the internet.

Using an attack strategy similar to a Rube Goldberg device where a complicated mix of many individual devices are used to perform a simple task, the hacker jumps from device to device until it hits the actual system or network it was targeting. Ang Chui, the CEO of the cyber security company Red Balloon, expands on this idea by stating, "We're looking at a fitness tracker hacking a smart speaker, a smart speaker hacking a thermostat, and the thermostat hacking the rest of the network. It's all laughs until that thermostat connects to a power plant or an embassy."[174] An attacker may no longer need to invest extensive resources into hacking a secure phone or computer. Instead, they could execute a chain of attacks on more vulnerable systems to get to their end goal. The future threat of offensive cyberspace operations will continue to grow with the advent of more effective attack methods and the greater number of vulnerabilities found within the IoT.

---

[172] Matt Powell, "5 Simple IoT Devices That Can Become Entry Points for Hackers," *CPO Magazine*, December 30, 2019, www.cpomagazine.com/tech/5-simple-iot-devices-that-can-become-entry-points-for-hackers/.

[173] Newman, "Elaborate Hack."

[174] Newman.

## C. OPSEC CONCERNS

In the past, attackers sought members of the opposing military to gain information about their future actions, but recently, their family members and friends have also become targets. In the future, the target of OPSEC vulnerabilities could even become the general public. The actions of Bellingcat in providing evidence that shows Russia shot down MH17 is an excellent example of this phenomenon of OSINT investigations targeted at the population and not just the military. The general population has little, if any, knowledge of OPSEC. Militaries with trained personnel have a hard-enough time keeping their troops from posting critical information online. The general populace with little or no training in information security is more vulnerable. With the increased number of sensors (wireless cameras, phone cameras, door cameras, etc.) that are connected every day, as well as free OSINT investigative training that people receive on collecting, the value of targeting the general populous for information becomes significantly more valuable.

Concerns with OPSEC will grow as the world continues to connect through the internet and more sensors (mobile phone cameras, wireless cameras, etc.) propagate homes, offices, transportation, public and private places. These changes to the information environment may make covert operations significantly more difficult. Bellingcat has illustrated the effectiveness of OSINT investigations to collect information and use it to track the Russian 53rd Anti-Aircraft Missile Brigade's movements through Ukraine. The ability of militaries to move without attracting attention will become increasingly difficult as the number of people installing wireless cameras and entryway sensors will continue to rise. A marketing study by Statistics Market Research Consulting showed a growth rate in the industry of 9.6%.[175] As more cameras propagate the world, there will be more sensors to view what is occurring. These additional sensors will make military movements harder to conceal. The rise of OSINT investigative training may become the next education fad within tech.

[175] "Wireless Security Cameras—Global Market Outlook (2017–2026)," Research and Markets, July 2019, www.researchandmarkets.com/reports/4827765/wireless-security-cameras-global-market-outlook?utm_source=dynamic&utm_medium=GNOM&utm_code=pqkx8z&utm_campaign=1336584+-+Wireless+Security+Cameras+World+Markets+to+2026&utm_exec=joca220gnomd.

Bellingcat offers workshops around the world on OSINT investigative techniques. These are five-day classes, where "the first two days will focus on investigations of videos and photographic content, and the third day will focus on social media investigation. The last two days allow the participant to apply those skills to topics of their choice, with assistance from the workshop leaders and Bellingcat team members."[176] Currently, Bellingcat offers these classes predominantly for journalists and members of Non-Governmental Organizations. Intelligence and military members are prohibited from attending. Furthermore, these classes are quite expensive; they are currently offered at 2,200 Euros per attendee. While this price may limit participation from some who are interested, Bellingcat offers free guides on its website. These guides cover topics like geolocation techniques for Google Earth, interpreting data from Strava's heatmaps, and a how-to guide for reverse image searches. The world may see a rise in OSINT investigators similar to the rise of hackers with the increase of mainstream home computer use. The increase of sensors and trained personnel to decipher and use that data will make military operations a challenge and increase the value of targeting the civilian population to create useful OPSEC exploits.

The intentional targeting of the general population with new malware promises to use phones in new ways to gather relevant intelligence information through OPSEC vulnerabilities. PlaceRaider is an example of malware that can be used to target the mobile phones of a country's population to conduct remote reconnaissance or "virtual theft" within physical spaces.[177] The hacker instructs the device to take a series of pictures from a cell phone and fits them together to create a complete image of a room or space. In essence, this malware turns a phone with a camera into a covert reconnaissance device. PlaceRaider collects images "using remote services on the mobile device. On board preprocessing performs gross data reduction and packaging for transmission. The model is generated off-

176 "New Bellingcat Workshops Announced for May–September 2020," Bellingcat, March 4, 2020, www.bellingcat.com/resources/events/2020/02/24/new-bellingcat-workshops-announced-for-may-september-2020/.

177 Robert Templeman, Zahid Rahman, David Crandall, and Apu Kapadia, "PlaceRaider: Virtual Theft in Physical Spaces with Smartphones," NDSS Symposium (2013): 1, https://www.ndss-symposium.org/ndss2013/ndss-2013-programme/placeraider-virtual-theft-physical-spaces-smartphones/.

board and is navigated with a tool that allows exploration in a realistic 3D environment that provides an easy method to mine the image set. The malicious actor can easily extract sensitive information."[178] The malware operates by taking random images with the infected device's own camera and then minimizes the file size to ease the transport of images back to a centralized location for examination. Coupling this form of malware with an IMSI catcher would allow the attacker to identify the location of different victims and then allow the malware to be triggered on victims' nearby areas of interest. Thus, as people walking by a targeted structure, the IMSI catcher could find their phone and the PlaceRaider application could be activated as the victim walks past. This form of malware would allow the targeting of certain areas or units from unsuspecting victims without risking any military assets. The use of malware on civilians to gain intelligence through OPSEC violation may be the next vulnerability of cellular and smartphones.

Ukraine has shown the dangers of OPSEC vulnerabilities by soldiers and their families when they have posted things to social media. These vulnerabilities were then exploited by reporters and OSINT investigators, like Bellingcat. The result was an embarrassment for Russia, as it was shown they had utilized troops in Ukraine and that a Russian unit shot down a Malaysian Airways jetliner. As the ordinary citizen becomes more connected and proficient with the digital technology around them, instead of targeting the opposing force, attackers may choose to target the unsuspecting populations for OPSEC vulnerabilities and use new technology to exploit them. Similar targeting shifts have been seen in the use of strategic bombing. Originally, aerial bombing was used against military targets, but then shifted to civilians in an effort to diminish the will to resist. It will be interesting to see what happens when a population realizes it is being exploited via its mobile devices. The bombing of London did not work for the Germans, the bombing of Japanese cities did little to wither the fighting spirit of the Japanese,[179] and the bombing

[178] Templeman, Rahman, Crandall, and Kapadia, "PlaceRaider," 4.

[179] Richard Overy, *Why the Allies Won* (London: Norton and Company, 1997), 132.

of Hanoi did little to curb the fighting in Vietnam.[180] How will the targeting of a population through cyberspace affect the outcome of a battle?

The future structure of tactical military intelligence may also change due to these new vulnerabilities. While some units operating in current conflict zones may be accustomed to signals intelligence personnel within their formations, the creation of new tactical level cyber soldiers in units may become the norm. The work pioneered by 1st Stryker Brigade of the 4th Infantry Division during their 2017 National Training Center (NTC) rotation shows the utility of a Cyber Reconnaissance team to scour OSINT looking for information on the enemy.

Since 1981, the U.S. Army has sent its Armored Brigade Combat Teams to NTC at Fort Irwin, California to fight the Opposing Force (OPFOR). The OPFOR, or 11th Armored Cavalry Regiment, is a specially designed Army unit to replicate possible threat forces.[181] The purpose of the unit is to create a cunning and effective enemy to ensure visiting units are prepared to face similar foes in the rigors of combat. In June of 2017, prior to arriving at Fort Irwin, the visiting unit, 1st Stryker Brigade Combat Team, 4th Infantry Division, created a "Cyber Reconnaissance team" in an attempt to outmaneuver and defeat the OPFOR.[182] The team was tasked with locating any pertinent information to defeat the OPFOR within the OSINT realm. While not every means to collect OSINT was available, the team used a variety of social media platforms (Facebook, Tinder, and Snapchat) as well as the Department of Defense media site, Dvidshub, to find relevant information.

---

[180] William S. Turley, *The Second Indochina War: A Concise Political and Military History* (Lanham, MD: Rowman & Littlefield, 2009), 132.

[181] 11th Armored Cavalry Regiment, accessed May 8, 2020, home.army.mil/irwin/index.php/units-tenants/11th-armored-cavalry-regiment.

[182] Christopher Lowman and Gerlad Prater, "Expansion of the Reconnaissance and Security BCT into the Cyber Domain: Lessons Learned from NTC Rotation 17-07.05" (unpublished white paper, July 2017), 1, cited in Curt Taylor, "It's Time for Cavalry to Get Serious about Cyber Reconnaissance," *Armor Mounted Maneuver Journal* (Fall 2018): 5–12, https://www.benning.army.mil/Armor/eARMOR/content/issues/2018/Fall/Fall2018_ARMOR_magazine.pdf.

Using OSINT analyzation techniques similar to Bellingcat, the Cyber Reconnaissance team scoured Dvidshub for useful information. Dvidshub is a collection of photos and videos from around the Department of Defense. By searching the database for the 11th Cavalry and then sifting through images and videos, the team identified key OPFOR leaders and weapon systems before the deployment to Fort Irwin began. Similar techniques proved valuable in establishing the OPFOR composition and hierarchy. Dvidshub contained enough relevant information to allow the Cyber Reconnaissance team to gain an understanding of the enemy, but it was collected passively and depended on what the OPFOR had posted to the website. To get actionable intelligence on the location of the OPFOR, the team had to become more proactive.

Throughout the course of the exercise, the team would locate the OPFOR and provide timely intelligence through the use of social media platforms. The two most effective platforms were Snapchat and Tinder. These applications are commonly used by young adults who are looking for partners. Snapchat is a photographic modification and communication application that can attach photos to a map so people nearby or around the world can view them.[183] Tinder is a dating application that uses geolocation to link possible matches.[184] These applications are especially popular with users between eighteen and twenty-four years of age, which make up a large portion of the military (35% of Tinder users[185] and 78% of Snapchat users[186] are between 18 and 24). The team created fake online personas for both applications that acted as "honey pots" to deceive targets and encouraged them to divulge relevant information. Members of the Cyber Reconnaissance team stated, "by creating a fake female Tinder profile and querying young Soldiers, we could collect important information pertaining to OPFOR units in the field. Information

183 "What Is Snapchat?" Snapchat, accessed May 8, 2020, whatis.snapchat.com/.

184 "What Is Tinder?" Tinder, accessed May 8, 2020, www.help.tinder.com/hc/en-us/articles/115004647686-What-is-Tinder-.

185 J. Clement, "U.S. Tinder Usage by Age 2018," Statista, November 26, 2019, www.statista.com/statistics/814698/share-of-us-internet-users-who-use-tinder-by-age/.

186 "Snapchat Statistics and Revenue: Snapchat by the Numbers," Influencer Marketing Hub, April 30, 2019, influencermarketinghub.com/snapchat-statistics-revenue/.

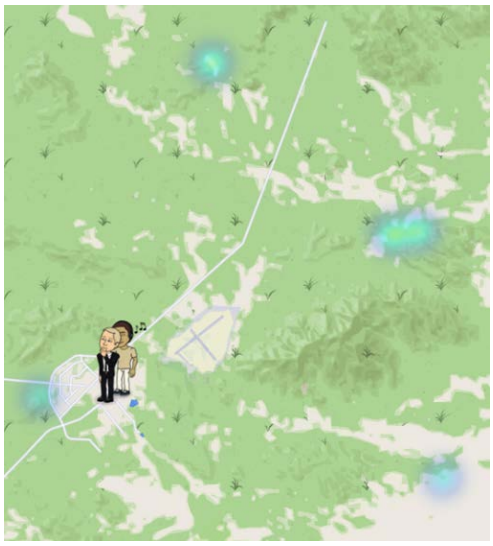
requested included unit affiliation, weapons, assets, and locations relative to the battlefield and terrain."[187]

Tinder was valuable for finding OPFOR locations because it automatically calculates the distance between the user and their match. By going to three previously known locations the Cyber Reconnaissance team triangulated their matches in the OPFOR. Over 100 soldiers in the OPFOR inadvertently contributed their location data which allowed for constant updates to their location. The one downside of this method is that Tinder rounds distance to the nearest whole mile. This created some ambiguity that was rectified with the assistance of Snapchat.

Snapchat introduced the Snap Map on 21 June 2017.[188] This feature allows a user to find another friended user precisely on a map. It also has a heat map feature, similar to the Strava health application, that shows the activity level of all the Snapchat users throughout the world. The heat map records activity over a twenty-four-hour period. In large cities these changes would be relatively minor. However, in the mostly desolate desert locale of Fort Irwin, California, the team was able to see the location and movements of OPFOR elements when the data was viewed over time (see Figure 13). The information collected by the Cyber Reconnaissance team allowed their unit to refine the locations of enemy forces, which assisted in the targeting and aided in the route selection of friendly forces.

[187] Lowman and Prater, "Expansion of the Reconnaissance and Security BC," 3.

[188] "Introducing Snap Map!" Snap, June 21, 2017, www.snap.com/en-US/news/page/4/.



This map shows the location of Snapchat activity (in blue and light green) which corresponds with OPFOR positions within the Fort Irwin, California, training area.

Figure 13. Snap Map from the Cyber Reconnaissance Team[189]

The ability to use social media to develop a common operating picture of the battlefield and find the location of enemy units is shocking. The same things that young adults are using to find possible mates in the civilian world are being used by military intelligence personnel to locate enemy units in the realm of battle. Members of the Cyber Reconnaissance team stated the achievements from their intelligence collecting techniques "were the result of flaws in operational security. Moving forward, we [the U.S. Military] must understand the gravity of OSINT."[190] Threats to OPSEC are all around. It should be clear that innocent devices and applications can have significant consequences to a well-motivated enemy. Vulnerabilities to OPSEC do not just come from phones and other devices; the human aspect is even more troublesome. Soldiers that gave away their position from carelessly looking at their phone and scrolling through Tinder and Snapchat had briefings and received training on OPSEC. The family members of these soldiers have received no such training. As shown by the family members of the 53rd Anti-Aircraft

[189] Source: Lowman and Prater, "Expansion of the Reconnaissance and Security BC," 4.

[190] Lowman and Prater, 8.

Missile Brigade, they are even riper for exploitation through their devices and ignorance. While a Cyber Reconnaissance team may prove less useful against a well-disciplined and modernized military, it would be very effective against less disciplined proxy forces. Then again, as this thesis has already explored, U.S. and Russian troops are quite susceptible to OPSEC traps through social media. Who is to say that Chinese or Iranian military personnel are any better?

The vulnerabilities from cellular and smartphones will continue to increase and have far-reaching effects for troops on the battlefield as well as the governments that deploy them and the citizens that support them. The effect of deepfake video combined with individualized information from previous cyberspace exploitation will most likely be significant in terms of creating effective propaganda to degrade combat forces. The rise of 5G will continue to allow attackers to exploit mobile networks with new methods. The IoT will become a more vulnerable pathway as more devices are connected. Each of these devices will then become a new attack vector allowing hackers to gain access to networks through a chain of easily exploited electronic gadgets. OPSEC will become harder to achieve as more cameras are added to the potential battlespace, as private individuals become more capable of collecting and deciphering OSINT information, and as the electronic signature of users through common applications are exploited to find their location. The target of OSINT collection may shift from the opposing military to the civilians of the opponent as they become better sensors than enemy troops. The vulnerabilities of cellular and smartphones on the battlefield is apparent. The next chapter will introduce some actions that can mitigate the effects of these devices upon troops in combat.

THIS PAGE INTENTIONALLY LEFT BLANK

# V. PRESCRIPTIVE MEASURES

In April of 2018, Jeff Bezos, the owner of Amazon and the wealthiest person in the world, had dinner with Mohammed bin Salman, the Crown Prince of Saudi Arabia. During that dinner, the two men exchanged phone numbers associated with their respective messaging application accounts on "WhatsApp."[191] The next month, Mr. Bezos received a WhatsApp message, originating from the Crown Prince, with a video file that had been modified with spyware. Several hours after receiving the message, "massive and (for Bezos' phone) unprecedented exfiltration of data from the phone began." [192] Saudi Arabia, during this time period, had also infiltrated the phones of several political activists, dissidents, and non-government organization workers who were vocal against the Saudi regime. Several months later, Mr. Bezos received a photo of a woman who bears a strong similarity to the woman with whom he was having an affair. The photo was sent to him months before this information was known publicly.[193] The United Nations investigation into the matter believed Saudi Arabia targeted Bezos due to his ownership of the *Washington Post* newspaper and its support of Jamal Khashoggi, who was an outspoken critic of, and later murdered by, the regime.[194] The phone of the world's wealthiest person, who presumably had some of the best security and cyber protection money can buy, was hacked. What then can be done to protect the average soldier, who has significantly fewer resources on the battlefield?

Threats to phones pose a severe vulnerability to the United States military. However, there are several ways to mitigate their effects. The most obvious solution is to prohibit all phones and other personally owned internet-attached devices for military

---

191 "UN Experts Call for Investigation into Allegations That Saudi Crown Prince Involved in Hacking of Jeff Bezos' Phone," OHCHR, January 22, 2020, www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=25488&LangID=E.

192 Avie Schneider and Shannon Bond, "U.N. Urges Probe of Reported Hacking of Jeff Bezos' Phone By Saudi Arabia," NPR, January 22, 2020, www.npr.org/2020/01/22/798457906/u-n-experts-urge-probe-of-reported-hacking-of-jeff-bezos-phone-by-saudi-arabia?utm_medium=RSS&utm_campaign=storiesfromnpr.

193 OHCHR, "UN Experts Call for Investigation."

194 OHCHR, "UN Experts Call for Investigation."

personnel. Another necessary step is to improve the education and training of service members as it relates to cellular and smartphone vulnerabilities. The user is the weakest link to any technical device, and the military needs to ensure its personnel understand the extent of these threats and are prepared to counter them. Finally, the United States military needs to ensure its partner forces and allies are aware of the vulnerabilities of phone use and are prepared to respond to the effects of these devices.

## A. BANNING PHONES

Cell phones and other mobile devices could simply be prohibited for troops who are deployed. By removing phones and other personal mobile devices, the threats and vulnerabilities they introduce are eliminated. The United States Army's 82d Airborne Division recently executed such a policy ahead of its short notice deployment to Kuwait in January 2020.[195] The 1st Brigade Combat Team of the 82d Airborne Division was to be sent to Kuwait due to escalating tensions between the United States and Iran following rocket attacks on American facilities and the elimination of Iranian Quds Force commander General Qassem Soleimani. The 82d Airborne Division Commander, Major General James Mingus, stated, "This is not the normal kind of deployment. The decision [to not bring personal electronic devices is] 100 percent an operational security and force protection measure."[196] The prohibition on personal electronic devices was to stem the flow of information leaking out about the deployment—preventing OPSEC violations. It was also conducted to protect soldiers from the effects of enemy cyberattacks—targets of cyberspace exploitation operations.

The 82d Airborne Division's decision to not bring personal electronic devices was most likely made based on a National Terrorism Advisory Bulletin, issued after the attack that killed Solemani. The bulletin stated, "Iran maintains a robust cyber program and can execute cyberattacks against the United States. Iran is capable, at a minimum, of carrying out attacks with temporary disruptive effects against critical infrastructure in the United

195 Kyle Rempfer, "No Cellphones, Laptops Were Allowed to Go with Army 82nd Paratroopers Deploying to Middle East," *Army Times*, January 7, 2020, www.armytimes.com/news/your-army/2020/01/06/no-cell-phones-laptops-were-allowed-to-go-with-82nd-paratroopers-deploying-to-middle-east/.

196 Rempfer, "No Cellphones."

States."[197] Iran's cyber threat was significant enough to ensure cell phones did not make it to the battlefield or any of the associated support bases for American troops.

Within the military, it is common to have a set of regulations to prevent troops from conducting certain activities while on deployment. The restrictions often focus on alcohol consumption, sexual activities, illicit substances, personal firearms, and often fall under General Order Number 1, Prohibited Activities for members of the Department of Defense.[198] In the future, it may be necessary to include cell phones and other electronic devices under this General Order. Failure to obey these restrictions results in a violation of the Uniform Code of Military Justice and can result in a significant punishment for the service member, such as a loss of rank, pay, and possible discharge from the military. The establishment of such a severe punishment may assist in persuading troops not to bring cellular and smartphones on deployments.

If this strict prohibition on phone use is enacted, the military must create an opportunity for troops to utilize the internet and other communications devices. The lessons from early in the Global War on Terror could be of value in this situation. Before the widespread use of cellular and smartphones, troops went to computer labs and call centers while deployed to a combat zone. These facilities were created as a joint venture between the Morale Welfare and Recreation (MWR) division of United States Army Europe (USAREUR) and the Space and Naval Systems Command (SPAWAR) Systems Center Atlantic-European Office (SPAWAR Europe).[199] Together, they built a satellite "network capable of supporting high volumes of voice, video and data traffic to help foster positive morale and troop welfare by connecting soldiers with their loved ones."[200] While not available at every base in the combat area and limited on bandwidth, it was something the

197 "National Terrorism Advisory System Bulletin—January 18, 2020," Department of Homeland Security, January 29, 2020, www.dhs.gov/ntas/advisory/national-terrorism-advisory-system-bulletin-january-18-2020#.

198 "General Order No. 1—Prohibited Activities for Soldiers," *New York Times*, November 4, 2009, www.nytimes.com/interactive/projects/documents/general-order-no-1-prohibited-activities-for-soldiers.

199 "Satellite Network Keeps Soldiers Close to Home," iDirect Government, January 3, 2019, https://www.idirect.net/resources/spawar-satellite-network-keeps-soldiers-close-to-home/.

200 iDirect Government.

service member could use to send emails, make phone calls, and pay bills. To ensure security, these facilities and their networks need to be hardened and protected from enemy cyber-attacks. Furthermore, troops will need to be trained in how to protect themselves in cyberspace. The computers being utilized will also need to be updated regularly and have proper virus protection software. The establishment of these facilities is essential for troops to remain in contact with those back home and to give them another means to communicate when their phones have been banned.

## B. EDUCATION AND TRAINING OF U.S. FORCES

As evidenced by the amount of YouTube firefight and military prank videos, younger troops are more inclined to bring devices into the field. As a result, the military needs to better train its individual troops and units on the dangers of phones and mobile devices. Currently, the Department of Defense uses the Information Assurance (IA) training to explain the danger of phones and other mobile devices to individuals, including service members, civilians and contractors. The training is conducted annually, through a program called the Cyber Awareness Challenge 2020.[201] This program introduces the trainee to Marty, a person ten years in the future, who warns them of an apocalyptic world caused by cybersecurity incidents.[202] Marty then instructs the trainee that they can change the future by becoming more aware of the cyber threats and best practices that exist to counter them. The training focuses on the areas of Spillage, Sensitive Information, and Malicious Code. As the trainee completes each module of the training, the cyber threat is diminished, indicating the future is becoming more secure. The training seems to focus on the use of computers in an office environment, while little information is provided on the threats to mobile devices. The Cyber Security Challenge did include the Strava fitness app case study for GPS tracking; however, it was several screens the trainee could easily click through and ignore. In addition, no tactical or combat situations were included in the training to enlighten trainees to threats that could affect them on the battlefield.

---

201 "Cyber Awareness Challenge," DoD Cyber Exchange, accessed May 8, 2020, public.cyber.mil/training/cyber-awareness-challenge/.

202 The Cyber Awareness Challenge training can be conducted, by anyone, at https://dl.dod.cyber.mil/wp-content/uploads/trn/online/cyber-awareness-challenge/launchPage.htm.

New IA training needs to educate individual troops on the perils of posting to social media and the effects of OSINT through those mediums. The training also needs to give examples of the exploitation methods used by possible combatants on cellular and smartphones. Vignettes could be great teaching tools for younger service members and their leadership. If troops understand the hazards their phones create for their squad, platoon, or unit, they might be less inclined to utilize them on patrol.

Unit field training needs to replicate the vulnerability of phone use and include direct consequences for their usage in these scenarios. Within the Army, there needs to be more emphasis on the effects of IW within the Combat Training Centers. These are the primary training events for Army Brigade Combat Teams that deploy to train against the OPFOR at Fort Irwin, California; Fort Polk, Louisiana; or Hohenfels, Germany. These training centers do an excellent job of stressing units and testing them in combined arms maneuver warfare, but they do little to introduce the threats and complexity demonstrated by Russian NGW and other asymmetric threats to the United States. Army Colonel Liam Collins states, "These scenarios tend to ignore or undervalue the role of information operations. To be sure, it is difficult to simulate many information operations effects in training or simulation, but that should not be the justification for ignoring them."[203] These facilities have a limited ability to jam tactical radio traffic, but that is the extent the IW effects used by the OPFOR. The Combat Training Centers need to do a better job of replicating the current threat for their trainees.

Currently, the training team and OPFOR at the Joint Readiness Training Center in Fort Polk, Louisiana, take cellular and smartphone use seriously. Fort Polk bans the use of personal phones by everyone in a visiting unit except for some essential leaders who need to have contact with elements back at their home location.[204] Those caught using their phones while in the training area are targeted with simulated artillery strikes. This policy

[203] Liam Collins, "Learning From Russia's Information Offensives," Association of the United States Army, October 24, 2018, www.ausa.org/articles/learning-russia%E2%80%99s-information-offensives.

[204] Joint Readiness Training Center, *Joint Readiness Training Center (JRTC) Exercise Rules of Engagement (EXROE) FY19* (Fort Polk, LA: Joint Readiness Training Center, December 2018).

replicates the many triangulation systems that exist to locate cellular phones and then target their users with lethal effects.

The United States Marine Corps also takes the dangers of cellular and smartphones seriously. This potential real-life scenario was recently depicted at a training exercise in California's Mojave Desert at Twentynine Palms.[205] A young Marine lance corporal took a selfie with his smartphone. The photo that he posted to social media was geotagged, which made known his unit type and location to the OPFOR. The Observer/Controller, or umpire, of the training event then "destroyed" the entire unit since proper targeting data could be rendered from the lance corporal's post. Lieutenant General Lori Reynolds, the Marine Corps' Deputy Commandant for Information, stated, "I'm sure that lance corporal was not happy. But it's OK to learn those things in Twentynine Palms—we don't want to learn those elsewhere."[206] This event surely gave the lance corporal's unit a "black eye" and caused everyone from the lowest Marine to the unit's Commander to learn a lesson. To be effective, these lessons from training need to have widespread and far-reaching effects to ensure troops and senior commanders understand the dangers of cellular and smartphones on the battlefield.

While the removal of units from the training scenario to mimic being destroyed in battle can be an effective teaching tool, more can be done to truly replicate the full spectrum of dangers from cellular and mobile phones. The hacking of actual wireless networks used by the civilian populace would be illegal and problematic; therefore, a new training network could be created and visiting units could be forced to communicate through it. The closed network could then be manipulated, disrupted, and even shut down. This would give the unit getting trained a better appreciation for the threats they may face without any interference to actual military networks or private systems. To fully replicate the effects of adversarial interference to mobile communications, the government phone of every key leader would be replaced with a "training phone." Each training center would maintain a

---

[205] Gina Harkins, "A Lance Corporal's Phone Selfie Got His Marine Unit 'Killed' at 29 Palms," Military.com, January 7, 2020, www.military.com/daily-news/2020/01/07/lance-corporals-phone-selfie-got-his-marine-unit-killed-29-palms.html.

[206] Harkins, "A Lance Corporal's Phone Selfie."

"training phone" for the critical brigade leaders that are reissued to each visiting unit. These phones would have generic contact data already uploaded to ease the burden of use. Furthermore, the "training phones" would operate on the enclosed network unique to the training center. This would allow the "training phones" to receive the same manipulations a phone in combat may experience. The use of dedicated "training phones" and networks would give leaders the experience of being hacked, spied on, and manipulated via their phone. Using OSINT investigating techniques, the OPFOR could even send threatening text messages to key leadership. The experience gained by unit leaders would go a long way in ensuring lower-level troops are better trained and have a better understanding of the dangers cellular and smartphones bring to the battlefield. Senior leaders could ensure that those in their chain of command are educated about enemy threats and the vulnerability of electronic devices. Instead of merely telling a service member not to bring their phone, the young soldier would now understand the "why" behind that decision. It will take significant funding and resources to make these training events work; however, their effects will go a long way in preparing U.S. troops and their leaders for the threats ahead.

## C. TRAINING AND EDUCATION FOR U.S. ALLIES AND PARTNER FORCES

The training of U.S. Allies and Partner Forces is essential to creating an effective deterrent to future conflict and preparing capable forces who are ready to fight in the event deterrence fails. U.S. Army Special Forces and the newly created Security Forces Assistance Brigades (SFAB) represent the two units the United States Army uses for conducting training with other nation's militaries. These units are specially trained and equipped to train others to fight. The main missions for Special Forces are foreign internal defense and unconventional warfare.[207] In these roles, Special Forces train friendly nation militaries and indigenous populations to conduct guerrilla warfare, respectively. However, as the current War on Terror has shown, the requirement to build up the army of Afghanistan and Iraq requires a significant amount of resources and trained professionals. General Miley, the former Chief of Staff of the Army, stated, "[Special Forces] can't really

[207] "Primary Special Forces Missions," Goarmy.com, accessed May 8, 2020, www.goarmy.com/special-forces/primary-missions.html.

train the scope and level of training of an entire national army. It fell to the regular Army to do it."[208] Furthermore, Special Forces did not have the ability to train these host nation's armies in job skills other than light infantry tactics. This left capability gaps in armor, artillery, logistics, and other vital skills for an army. The requirement to train entire armies meant the United States needed to create new units.

The creation of the Security Force Assistance Command is a direct result of this requirement to train national armies. The current Security Force Assistance Command oversees five active-duty Security Force Assistance Brigades and one National Guard Brigade to train partner forces and their national armies.[209] The purpose of these units is "to conduct training, advising, assisting, enabling, and accompanying operations with allied and partner nations."[210] Furthermore, these unique units are made up of soldiers who "are highly trained, and among the top tactical leaders in the Army. Their work will strengthen our allies and partners while supporting this Nation's security objectives and the combatant commanders' warfighting needs."[211] These Brigades exist solely to train and assist other nations in conducting and preparing for combat operations. There is one dangerous pitfall in the organizational structure of these units: no information security or IW capability. As IW has proven to be an effective component of modern battle, to stay effective in current and future fights, the United States needs to expand IW and IA training to its allies and partner forces.

An information component needs to be added to the SFAB in order to improve its effectiveness as trainers, but the current number of IW personnel in these units is not sufficient for training this function. SFABs currently recruit from a large array of military occupational specialties from within the Army, but they do not include many soldiers who

---

208 Meghann Myers, "Army Chief: SFABs Will Do a Completely Different Job than Special Forces," *Army Times*, October 31, 2017, www.armytimes.com/news/your-army/2017/10/31/army-chief-sfabs-will-do-a-completely-different-job-than-special-forces/.

209 "U.S. Army Forces Command: SFAC," Army.mil, accessed May 8, 2020, www.army.mil/sfac#org-about.

210 "Security Force Assistance Brigade (SFAB)," Goarmy.com, accessed May 8, 2020, www.goarmy.com/careers-and-jobs/current-and-prior-service/advance-your-career/security-force-assistance-brigade.html.

211 Goarmy.com, "Security Force Assistance Brigade (SFAB)."

specialize in an information related capability. The Army manual on Security Force Assistance Brigades states, "The SFAB has a sparse information capability that does not include specialists outside of communications technicians."[212] Members of the SFAB headquarters include Psychological Operations, Civil Affairs, and Electronic Warfare experts. However, these personnel are all senior Non-Commissioned Officers or mid-career Commissioned Officers whose job is to assist with planning. This small number of personnel is not sufficient to create effective training for a host nation army. Furthermore, the individual advisor teams have no IW experts in their formation which is ineffective because they are the ones who actually interact with the trainees. To be more effective, these organizations need to create a more diverse IW component made up of Psychological Operations, Information Operations, Cyber, and more Electric Warfare professionals. The IW component could be a part of the Brigade Headquarters Company so they can train the individual advisor teams and be used as trainers for special situations. With an effective IW component, the SFAB will be considerably more capable of preparing host-nation armies to face credible future threats.

The United States does not need to stand alone in the effort to train forces on the dangers of cellular and smartphones. This training and education model could be expanded to include NATO forces as well. It might be best if European Command, in conjunction with NATO, were to create an Information Warfare Taskforce. Basing the Taskforce in Estonia would be logical since it is home to the Tallinn Cyber Center of Excellence.[213] This center was developed after cyber-attacks Estonia experienced at the hands of Russia in 2007. Tallinn has become the focal point of cyber defense and warfare understanding within NATO. Thus, they have a more credible presence when working with NATO allies and other European countries. With this experience and these resources, a Taskforce from the Cyber Center of Excellence could be instrumental in training eastern European

212 Department of the Army, *Security Force Assistance Brigade*, ATP 3-96.1 (Washington, DC: Department of the Army, May 2018), 8-4.

213 "About Us." NATO Cooperative Cyber Defense Centre of Excellence, accessed May 8, 2020, ccdcoe.org/about-us/.

countries and fostering a more secure mindset in regard to IW, cybersecurity, IA, and the use of cellular and smartphones.

This change in mindset regarding cybersecurity and smartphone use is not only necessary in Europe, but around the globe. As China moves to push its 5G technology on the world, the threat of data exploitation is has become far greater. This poses a significant strategic threat to the United States and its allies. However, this technology also poses a substantial tactical threat. As has been illustrated earlier in this thesis and throughout history, when an adversary can read an opponent's secret messages, the opponent loses a significant advantage. With this threat in mind, our partners and allies in the Pacific need to ensure they practice effective IA, OPSEC, and are aware of the threats from cellular and smartphones. The United States has traditionally conducted annual training exercises in South Korea, Thailand, and the Philippines. These training events should also include IW scenarios. American combat elements that deploy to these areas and their associated command structures need to gain more repetitions in training against these threats. Furthermore, American allies in Asia, particularly because of the Chinese threat, also need to be prepared for these same risks.

## D. CONCLUSION

It is going to be very difficult to remove mobile phones from each soldier. When research teams in Ukraine interviewed troops on why they continued to use their phones despite their vulnerabilities, they stated: "We need to live."[214] They need to stay connected to their families, pay their bills, and have fun on their off time. With effective prescriptive measures, troops can gain a better understanding of how the devices they "need to live" can actually help them die in combat. If each service member understands the dangers of his devices and if he has effective leadership to keep these devices controlled, then the threat can become significantly reduced.

[214] Aaron Brantly, "Defending the Borderlands of Europe: Ukrainian and American Experience with IO, Cyber and EW," lecture, May 16, 2019, Defense Analysis Program, Naval Postgraduate School, Monterey, CA.

The prescriptive measures discussed in this chapter could be very effective in mitigating the vulnerabilities introduced by the use of cellular and smartphones to the battlefield. Improved training and education for troops at the individual level will make them more aware of the dangers that come from mobile devices. The collective unit training they experience at the Combat Training Centers with dedicated training networks and phones can take lessons learned in a classroom and transform them into tangible experiences to cement those lessons. Finally, by improving the units that train American allies and partner forces with the addition of information detachments, the United States can ensure its friends and compatriots around the world are better able to fight and win on the battlefield of the future in which the exploitation of technology will take on a key role.

This thesis serves to give an understanding of how cellular and smartphones introduce vulnerabilities to the battlefield that make it easier for the enemy to exploit the American warfighter. This began with a look at the operation of cellular phones, networks, and IMSI catchers to allow the reader to understand how these devices work. With this technical understanding, the reader was introduced to the three vulnerabilities created by cellular and smartphones: propaganda proliferation, targets of cyberspace exploitation, and OPSEC concerns. These vulnerabilities were discussed through the case study of the 2014 Russian invasion and subsequent occupation of eastern Ukraine. The case study allowed the reader to experience the effects of these vulnerabilities in a real-world scenario. Each of the vulnerabilities was then examined through a recent incident that had direct effects on the United States military to emphasize the threat of these devices. Next, the thesis examined the future of these three vulnerabilities on the United States military. The development of 5G technology, deepfake videos, and vulnerabilities in the IoT all offer new vectors to attack and exploit American service members. Finally, the thesis concludes with a look at some prescriptive measures to mitigate the damage from cellular and smartphones. While banning phones is the easiest to implement, more effective training and education is needed to ensure service members know the reason why their phones cannot be used. This model then needs to be applied to the allies and partner forces of the United States. Ensuring the warfighter knows why his/her phone is a hazard is the key to preventing it from causing harm in battle.

The weaponization of technology will continue to increase as technology advances and as hackers have more time to exploit its vulnerabilities. The battlefield will become a more chaotic place as violence and technology merge to make combat faster and more deadly. The Ukrainian case study shows many of the battlefield vulnerabilities opened by the widespread use of cellular phones. No longer do commanders need merely to concern themselves with embarrassing photos and messages written by soldiers on social media. The war in Ukraine is only a glimpse of what is in store for the global community in the remainder of the twenty-first century. Commanders need to realize that the devices that have brought the internet to everyone's fingertips can also bring the enemy. Innocent applications that allow family members to track everyone's location can be manipulated to deliver lethal artillery rounds. The photo sent from a soldier's wife to her husband can now be sent to a false cell tower, uploaded with malware and sent to a victim to attack their phone or target their location. The United States needs to be prepared to defeat its foes and extend a helping hand to allies, both on the physical battlefield and in the information environment.

# LIST OF REFERENCES


Al Agha, Khaldoun, Guy Pujolle, and Tara Ali-Yahiya. *Mobile and Wireless Networks*, vol. 2. Hoboken, NJ: Wiley, 2016. https://doi.org/10.1002/9781119007548.

American Civil Liberties Union. "Stingray Tracking Devices." Accessed May 3, 2020. www.aclu.org/issues/privacy-technology/surveillance-technologies/stingray-tracking-devices.

Army.mil. "U.S. Army Forces Command: SFAC." Accessed May 8, 2020. www.army.mil/sfac#org-about.

Barrett, Devlin. "Americans' Cellphones Targeted in Secret U.S. Spy Program." *Wall Street Journal*, November 14, 2014. www.wsj.com/articles/americans-cellphones-targeted-in-secret-u-s-spy-program-1415917533.

BBC. "MH17 Ukraine Plane Crash: What We Know." February 26, 2020. www.bbc.com/news/world-europe-28357880.

Bellingcat. "New Bellingcat Workshops Announced for May–September 2020." March 4, 2020. www.bellingcat.com/resources/events/2020/02/24/new-bellingcat-workshops-announced-for-may-september-2020/.

———. "Origin of the Separatists' Buk: A Bellingcat Investigation." November 18, 2014. www.bellingcat.com/news/uk-and-europe/2014/11/08/origin-of-the-separatists-buk-a-bellingcat-investigation/.

Bellware, Kim, and Kayla Epstein. "Did You Get 'Drafted' by the U.S. Army via Text Message? It's a Hoax." *Washington Post*, January 8, 2020. www.washingtonpost.com/national-security/2020/01/08/army-draft-text-message-hoax/#comments-wrapper.

Bērziņš, Jānis. "Russia's New Generation Warfare in Ukraine: Implications for Latvian Defense Policy." Policy paper, National Defence Academy of Latvia Center for Security and Strategic Research 2014.

Brandom, Russell. "Phony Cell Towers Are the Next Big Security Risk." The Verge, September 18, 2014. www.theverge.com/2014/9/18/6394391/phony-cell-towers-are-the-next-big-security-risk.

Brantly, Aaron. "A Bear of a Problem: Russian Special Forces Perfecting Their Cyber Capabilities." Association of the United States Army, November 28, 2018. www.ausa.org/articles/bear-problem-russian-special-forces-perfecting-their-cyber-capabilities.

Brown, Daniel. “Russian-Backed Separatists Are Using Terrifying Text Messages to Shock Adversaries—And It’s Changing the Face of Warfare.” *Business Insider*, August 14, 2018. www.businessinsider.com/russians-use-creepy-text-messages-scare-ukrainians-changing-warfare-2018-8.

Chesney, Robert, and Danielle K Citron. “Disinformation on Steroids: The Threat of Deep Fakes.” Council on Foreign Relations, October 16, 2018. www.cfr.org/report/deep-fake-disinformation-steroids.

Clark, Robert M. *Intelligence Collection*. Los Angeles, CA: SAGE, 2014.

Clement, J. “U.S. Tinder Usage by Age 2018.” Statista, November 26, 2019. www.statista.com/statistics/814698/share-of-us-internet-users-who-use-tinder-by-age/.

Collins, Liam. “Learning from Russia’s Information Offensives.” Association of the United States Army, October 24, 2018. www.ausa.org/articles/learning-russia%E2%80%99s-information-offensives.

———. “Russia Gives Lessons in Electronic Warfare.” Association of the United States Army, July 26, 2018. https://www.ausa.org/articles/russia-gives-lessons-electronic-warfare.

Corfield, Gareth. “Latest 4G, 5G Phone-Location Slurp Attack Is a Doozy, but Won’t Torpedo Average Joe or Jane.” The Register, February 26, 2019. www.theregister.co.uk/2019/02/26/torpedo_piercer_attacks/.

CrowdStrike. “Use of Fancy Bear Android Malware in the Targeting of Ukrainian Field Artillery Units.” December 22, 2016. https://www.crowdstrike.com/resources/reports/idc-vendor-profile-crowdstrike-2.

Dabrowski, Adrian, Nicola Pianta, Thomas Klepp, Martin Mulazzani, and Edgar Weippl, “IMSI—Catch Me If You Can: IMSI-Catcher-Catchers,” *Proceedings of the 30th Annual Computer Security Applications Conference* (2014): 246–55, https://doi.org/10.1145/2664243.2664272.

Department of the Army. *Field Artillery Manual Cannon Gunnery*. TC 3–09.81 Washington, DC: Department of the Army, April 2016. https://armypubs.army.mil/epubs/DR_pubs/DR_a/pdf/web/tc3_09x81.pdf.

———. *Security Force Assistance Brigade*. ATP 3-96.1. Washington, DC: Department of the Army, May 2018.

Department of Homeland Security. “National Terrorism Advisory System Bulletin—January 18, 2020.” January 29, 2020. www.dhs.gov/ntas/advisory/national-terrorism-advisory-system-bulletin-january-18-2020#.

Deyan G. “60 Revealing Statistics about Smartphone Usage in 2020.” Tech Jury, January 9, 2020. techjury.net/stats-about/smartphone-usage/#gref.

DoD Cyber Exchange. “Cyber Awareness Challenge.” Accessed May 8, 2020. public.cyber.mil/training/cyber-awareness-challenge/.

Foreign Military Studies Office. “Counter UAV Tactics and the ‘Leer-3’ Electronic Warfare System.” *OE Watch* 7, no. 7 (August 2017): 3.

———. “Russia’s UAV Virtual Cellular Communication Tower.” *OE Watch* 7 no. 2 (March 2017): 54.

Fung, Brian. “How China’s Huawei Took the Lead over U.S. Companies in 5G Technology.” *Washington Post*, April 10, 2019. www.washingtonpost.com/technology/2019/04/10/us-spat-with-huawei-explained/.

Galeotti, Mark. “The ‘Gerasimov Doctrine’ and Russian Non-linear War.” In Moscow’s Shadows, September 17, 2017. inmoscowsshadows.wordpress.com/2014/07/06/the-gerasimov-doctrine-and-russian-non-linear-war/.

———. *Russian Political War: Moving beyond the Hybrid*, 1st ed. Abingdon, UK: Routledge, 2019.

Gallagher, Ryan. “Meet the Machines That Steal Your Phone’s Data.” Ars Technica, September 25, 2013. arstechnica.com/tech-policy/2013/09/meet-the-machines-that-steal-your-phones-data/.

Gartzke, Erik, and Jon R. Lindsay. “Weaving Tangled Webs: Offense, Defense, and Deception in Cyberspace.” *Security Studies* 24 (2015): 316–48. https://doi.org/1080/09636412.2015.1038188.

Giles, Keir. *The Next Phase of Russian Information Warfare*. Riga, Latvia: NATO Strategic Communications Centre of Excellence, 2016. https://www.stratcomcoe.org/next-phase-russian-information-warfare-keir-giles.

Goarmy.com. “Primary Special Forces Missions.” Accessed May 8, 2020. www.goarmy.com/special-forces/primary-missions.html.

———. “Security Force Assistance Brigade (SFAB).” Accessed May 8, 2020. www.goarmy.com/careers-and-jobs/current-and-prior-service/advance-your-career/security-force-assistance-brigade.html.

Greenberg, Andy. *Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin’s Most Dangerous Hackers*. New York, NY: Random House, 2019.

Grohmann, Karolos. “Russia Banned from Pyeongchang Winter Olympics.” Reuters, December 6, 2017. www.reuters.com/article/us-olympics-2018-russia/russia-banned-from-pyeongchang-winter-olympics-idUSKBN1DZ2QZ.

*Guardian*. “Malaysia Airlines MH17 Crash: What We Know So Far.” July 18, 2014. www.theguardian.com/world/2014/jul/18/mh17-crash-what-we-know-so-far-malaysia-airlines-ukraine.

Halpern, Sue. “The Terrifying Potential of 5G Technology.” *New Yorker*, April 30, 2019. www.newyorker.com/news/annals-of-communications/the-terrifying-potential-of-the-5g-network.

Heisler, Yoni. “Mobile Internet Usage Surpasses Desktop Usage for the First Time in History.” BGR, November 2, 2016. bgr.com/2016/11/02/internet-usage-desktop-vs-mobile/.

Harkins, Gina. “A Lance Corporal’s Phone Selfie Got His Marine Unit ‘Killed’ at 29 Palms.” Military.com, January 7, 2020. www.military.com/daily-news/2020/01/07/lance-corporals-phone-selfie-got-his-marine-unit-killed-29-palms.html.

Harwell, Drew, and Tony Romm. “U.S. Government Investigating TikTok over National Security Concerns.” *Washington Post*, November 1, 2019. www.washingtonpost.com/technology/2019/11/01/us-government-investigating-tiktok-over-national-security-concerns/.

Howard, Colby, and Ruslan Pukhov (eds.). *Brothers Armed: Military Aspects of the Crisis in Ukraine*, 2nd ed. Minneapolis, MN: East View Press, 2015.

Hussain, Syed, Rafiul, Mitziu Echeverria, Omar Chowdhury, Ninghui Li, and Elisa Bertino. “Privacy Attacks to the 4G and 5G Cellular Paging Protocols Using Side Channel Information,” NDSS Symposium (2019. https://www.ndss-symposium.org/ndss-paper/privacy-attacks-to-the-4g-and-5g-cellular-paging-protocols-using-side-channel-information/.

Ibe, Oliver C. *Fundamentals of Data Communication Networks.* Hoboken, NJ: Wiley, 2017.

IDF, “How Is the IDF Minimizing Harm to Civilians in Gaza?” July 16, 2014. www.idf.il/en/articles/hamas/how-is-the-idf-minimizing-harm-to-civilians-in-gaza/.

iDirect Government. “Satellite Network Keeps Soldiers Close to Home.” January 3, 2019. https://www.idirect.net/resources/spawar-satellite-network-keeps-soldiers-close-to-home/.

Influencer Marketing Hub. “Snapchat Statistics and Revenue: Snapchat by the Numbers.” April 30, 2019. influencermarketinghub.com/snapchat-statistics-revenue/.

Inform Napalm. “Russian Leer-3 EW System Revealed in Donbas.” September 25, 2016. informnapalm.org/en/russian-leer-3wf-donbas/.

Ismail, Nick. “Common Security Vulnerabilities of Mobile Devices.” Information Age, February 21, 2017. www.information-age.com/security-vulnerabilities-mobile-devices-123464616/.

Jaitner, Margarita L. “Russian Information Warfare: Lessons from Ukraine.” In *Cyber War in Perspective: Russian Aggression against Ukraine*, ed. Kenneth Greers. Tallinn: NATO Cooperative Cyber Defense Centre of Excellence, 2015.

Johnson, Cameron. “What Is PSTN and How Does it Actually Work?” Nextiva, April 4, 2019. www.nextiva.com/blog/what-is-pstn.html.

Joint Chiefs of Staff. *Cyberspace Operations*, JP 3-12. Washington, DC: Joint Chiefs of Staff.

Joint Readiness Training Center. *Joint Readiness Training Center (JRTC) Exercise Rules of Engagement (EXROE) FY19*. Fort Polk, LA: Joint Readiness Training Center, December 2018.

Just Ask Gemalto. “Generations of Mobile Networks: Explained.” August 2, 2018. www.justaskgemalto.com/us/ generations -mobile-networks-explained/.

Kelly. “Why Do We Use The Term Cellular Phone Instead of Mobile Phone?” Gizmodo, June 17, 2013. gizmodo.com/why-do-we-use-the-term-cellular-phone-instead-of-mobile-5840939.

Kesling, Ben, and Georgia Wells. “U.S. Military Bans TikTok over Ties to China.” Dow Jones Institutional News, January 3, 2020. http://libproxy.nps.edu/login?url=https://search.proquest.com/docview/2332264634?accountid=12702.

Kremlin. “Direct Line with Vladimir Putin.” April 16, 2015. http://en.kremlin.ru/events/president/news/49261.

Kumar, Arun, Arun Prasath, Gowtham K, and Meenachi Sundram. “Mobile Phones: History and Growth.” *EPRA International Jouranl of Research and Development* 4, no. 3 (March 2019): 44–48. https://eprajournals.com/jpanel/upload/837pm_11.Arun%20Kumar%20S-3013-1.pdf.

Kumar, Mohit. “New Attacks against 4G, 5G Mobile Networks Re-Enable IMSI Catchers.” Hacker News, February 25, 2019. thehackernews.com/2019/02/location-tracking-imsi-catchers.html.

Lally, Kathy. “Ukraine, Short on Military Budget, Starts Fundraising Drive.” *Washington Post*, April 19, 2014. www.washingtonpost.com/world/europe/ukraine-short-on-military-budget-starts-fundraising-drive/2014/04/19/0eba04d0-c7f6-11e3-8b9a-8e0977a24aeb_story.html.

Li, Zhenhua, Weiwei Wang, Christo Wilson, Jian Chen, Chen Qian, Taeho Jung, Lan Zhang, Kebin Liu, Xiangyang Li, and Yunhao Liu. “FBS-Radar: Uncovering Fake Base Stations at Scale in the Wild.” Paper presented at the NDSS Symposium 2017. https://doi.org/10.14722/ndss.2017.23098.

Libicki, Martin C. *What Is Information Warfare?* Washington, DC: National Defense University, Institute for National Strategic Studies, 1995.

Lippman, Daniel. “Israel Accused of Planting Mysterious Spy Devices near the White House.” *POLITICO*, September 12, 2019. www.politico.com/story/2019/09/12/israel-white-house-spying-devices-1491351.

Littell, Joe. “Don’t Believe Your Eyes (or Ears): The Weaponization of Artificial Intelligence, Machine Learning, and Deepfakes.” War on the Rocks, October 7, 2019. warontherocks.com/2019/10/dont-believe-your-eyes-or-ears-the-weaponization-of-artificial-intelligence-machine-learning-and-deepfakes/.

Lookout. “Monokle: The Mobile Surveillance Tooling of the Special Technology Center.” Research report, Lookout, July 2019. https://www.lookout.com/documents/threat-reports/lookout-discovers-monokle-threat-report.pdf.

Lowman, Christopher, and Gerald Prater. “Expansion of the Reconnaissance and Security BCT into the Cyber Domain: Lessons Learned from NTC Rotation 17–07.05.” Unpublished white paper, July 2017.

McElroy, Gil. “A Short History of the Handheld Transceiver.” *QST* (January 2005): 45–50. https://web.archive.org/web/20060220092549/http://www2.arrl.org/qst/2005/01/0501047.pdf.

McKew, Molly K. “The Gerasimov Doctrine: It’s Russia’s New Chaos Theory of Political Warfare. And It’s Probably Being Used on You.” *POLITICO*, September 10, 2017. https://www.politico.eu/article/new-battles-cyberwarfare-russia/.

Myers, Meghann. “Army Chief: SFABs Will Do a Completely Different Job than Special Forces.” *Army Times*, October 31, 2017. www.armytimes.com/news/your-army/2017/10/31/army-chief-sfabs-will-do-a-completely-different-job-than-special-forces/.

Nakashima, Ellen. “Hacks of OPM Databases Compromised 22.1 Million People, Federal Authorities Say.” *Washington Post*, July 10, 2015. www.washingtonpost.com/news/federal-eye/wp/2015/07/09/hack-of-security-clearance-system-affected-21-5-million-people-federal-authorities-say/.

———. “Russian Spies Hacked the Olympics and Tried to Make it Look like North Korea Did it, U.S. Officials Say.” *Washington Post*, February 24, 2018. www.washingtonpost.com/world/national-security/russian-spies-hacked-the-olympics-and-tried-to-make-it-look-like-north-korea-did-it-us-officials-say/2018/02/24/44b5468e-18f2-11e8-92c9-376b4fe57ff7_story.html.

NATO, “Member Countries.” June 9, 2017. www.nato.int/cps/en/natohq/topics_52044.htm.

———. “Russia Relations: The Facts.” July 9, 2016. www.nato.int/cps/en/natohq/topics_111767.htm#cl410.

———. “Study on NATO Enlargement.” November 5, 2008. www.nato.int/cps/en/natohq/official_texts_24733.htm.

Naylor, Sean. *Relentless Strike: The Secret History of Joint Special Operations Command*. New York, NY: St. Martin’s, 2015.

New Jersey Cybersecurity and Communications Integration Cell. “X-Agent.” February 16, 2017. www.cyber.nj.gov/threat-profiles/trojan-variants/x-agent.

Newman, Lily Hay. “An Elaborate Hack Shows How Much Damage IoT Bugs Can Do.” Wired, December 10, 2018. www.wired.com/story/elaborate-hack-shows-damage-iot-bugs-can-do/.

*New York Times*. “General Order No. 1—Prohibited Activities for Soldiers.” November 4, 2009. www.nytimes.com/interactive/projects/documents/general-order-no-1-prohibited-activities-for-soldiers.

OHCHR. “UN Experts Call for Investigation into Allegations That Saudi Crown Prince Involved in Hacking of Jeff Bezos’ Phone.” January 22, 2020. www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=25488&LangID=E.

Office of the Director of National Intelligence. “Background to ‘Assessing Russian Activities and Intentions in Recent U.S. Elections’: The Analytic Process and Cyber Incident Attribution.” Washington, DC: National Intelligence Council, 2017.

Ooi, Joseph. “IMSI Catchers and Mobile Security.” Capstone thesis, University of Pennsylvania, 2015. https://www.cis.upenn.edu/wp-content/uploads/2019/08/EAS499Honors-IMSICatchersandMobileSecurity-V18F.pdf.

Ostrovsky, Simon. “Russia Denies That its Soldiers Are in Ukraine, But We Tracked One There Using His Selfies.” Vice, June 16, 2015. www.vice.com/en_us/article/ev9dbz/russia-enies-that-its-soldiers-are-in-ukraine-but-we-tracked-one-there-using-his-selfies.

Overy, Richard. *Why the Allies Won*. London: Norton and Company, 1997.

Parasol, Max. “The Impact of China’s 2016 Cyber Security Law on Foreign Technology Firms, and on China’s Big Data and Smart City Dreams.” *Computer Law & Security Review* 34, no. 1 (February 2019): 67–98. https://doi.org/10.1016/j.clsr.2017.05.022.

Person, Robert. “Russian Grand Strategy in the 21st Century,” in *Russian Strategic Intention: A Strategic Multilayer Assessment (SMA) White Paper*, ed. Nicole Peterson, 7–13. Boston, MA: NSI, May 2019.

Political Geography Now. “Ukraine War Control Map & Report: June 2016.” June 2016. https://www.polgeonow.com/2016/06/ukraine-war-control-map-report-june-2016.html.

Powell, Matt. “5 Simple IoT Devices That Can Become Entry Points for Hackers.” *CPO Magazine*, December 30, 2019. www.cpomagazine.com/tech/5-simple-iot-devices-that-can-become-entry-points-for-hackers/.

Rempfer, Kyle. “No Cellphones, Laptops Were Allowed to Go with Army 82nd Paratroopers Deploying to Middle East.” *Army Times*, January 7, 2020. www.armytimes.com/news/your-army/2020/01/06/no-cell-phones-laptops-were-allowed-to-go-with-82nd-paratroopers-deploying-to-middle-east/.

Research and Markets. “Wireless Security Cameras—Global Market Outlook (2017–2026).” July 2019. www.researchandmarkets.com/reports/4827765/wireless-security-cameras-global-market-outlook?utm_source=dynamic&utm_medium=GNOM&utm_code=pqkx8z&utm_campaign=1336584+-+Wireless+Security+Cameras+World+Markets+to+2026&utm_exec=joca220gnomd.

Roache, Madeline. “Inside the Complicated Relationship Between Russia and NATO.” *Time*, April 4, 2019. time.com/5564207/russia-nato-relationship/.

Romein, Daniel. *MH17—Potential Suspects and Witnesses from the 53rd Anti-Aircraft Missile Brigade: A Bellingcat Investigation*. Bellingcat, 2016.

Roumeliotis, Greg. “Exclusive: U.S. Opens National Security Investigation into TikTok.” Reuters, November 4, 2019. www.reuters.com/article/us-tiktok-cfius-exclusive/exclusive-u-s-opens-national-security-investigation-into-tiktok-sources-idUSKBN1XB4IL.

Sanders, Deborah. “‘The War We Want; The War That We Got’: Military Reform and the Conflict in the East.” *Journal of Slavic Military Studies* 30, no. 1 (2017): 30–49.

Satter, Raphael. “Did CrowdStrike Really Miss the Mark?” Medium, July 20, 2018. medium.com/@rsatter/did-crowdstrike-really-miss-the-mark-ecedf0e09dd7.

———. “IMSI Catchers in Ukraine.” Google Docs, accessed May 11, 2020. https://docs.google.com/spreadsheets/d/1wnP1e-SS9_ArGX3M-miimJt-4SgmtSbUTraU10WMJKI/edit#gid=1560509081.

———. “Ukraine Soldiers Bombarded by ‘Pinpoint Propaganda’ Texts.” Associated Press, May 11, 2017. apnews.com/9a564a5f64e847d1a50938035ea64b8f/Sinister-text-messages-reveal-high-tech-front-in-Ukraine-war.

———. “‘You’re Just Meat’—Ukrainian Soldiers Get Chilling Texts.” May 11, 2017. apnews.com/1096d53b7e5a4a9682d6b434021fb2f8.

Sazonov, Vladimir, and Holger Mölder. “Why Did Russia Attack Ukraine?” *ENDC Occasional Papers* 6 (2017): 28–33.

Schneider, Avie, and Shannon Bond. “U.N. Urges Probe of Reported Hacking of Jeff Bezos’ Phone By Saudi Arabia.” NPR, January 22, 2020. www.npr.org/2020/01/22/798457906/u-n-experts-urge-probe-of-reported-hacking-of-jeff-bezos-phone-by-saudi-arabia?utm_medium=RSS&utm_campaign=storiesfromnpr.

Schogol, Jeff. “The Pentagon Has Declared War on...*Checks Notes*... Tik Tok.” Task & Purpose, December 19, 2019. taskandpurpose.com/news/dod-uninstall-tik-tok.

Shermeta, Bozhena. “Stuck in 2G, Moving to 3G as Other Nations Zoom to 4G.” *Kyiv Post*, May 29, 2015. kyivpost.com/article/content/doing-business-in-ukraine/stuck-in-2g-moving-to-3g-as-other-nations-zoom-to-4g-390959.html.

Sly, Liz. “U.S. Soldiers Are Revealing Sensitive and Dangerous Information by Jogging.” *Washington Post*, January 29, 2018. www.washingtonpost.com/world/a-map-showing-the-users-of-fitness-devices-lets-the-world-see-where-us-soldiers-are-and-what-they-are-doing/2018/01/28/86915662-0441-11e8-aa61-f3391373867e_story.html.

Snap. “Introducing Snap Map!” June 21, 2017. www.snap.com/en-US/news/page/4/.

Strava. “Features.” Accessed May 8, 2020. www.strava.com/features.

———. “The Global Heatmap.” Accessed May 8, 2020. www.strava.com/heatmap#8.69/44.72259/33.44340/hot/all.

Techopedia. “What Is International Mobile Subscriber Identity (IMSI)?” Last updated November 15, 2016. www.techopedia.com/definition/5067/international-mobile-subscriber-identity-imsi.

———. “What Is a Mobile Switching Center (MSC)?” Accessed May 3, 2020. www.techopedia.com/definition/8448/mobile-switching-center-msc.

Templeman, Robert, Zahid Rahman, David Crandall, and Apu Kapadia. “PlaceRaider: Virtual Theft in Physical Spaces with Smartphones.” NDSS Symposium (2013). https://www.ndss-symposium.org/ndss2013/ndss-2013-programme/placeraider-virtual-theft-physical-spaces-smartphones/.

Toler, Aric. “Russia’s ‘Anti-Selfie Soldier Law’: Greatest Hits and Implications.” Bellingcat, February 21, 2019. https://www.bellingcat.com/news/uk-and-europe/2019/02/20/russias-anti-selfie-soldier-law-greatest-hits-and-implications/.

Tucker, Patrick. “Russian Hackers Build Fake Skype, Signal, Pornhub Apps to Lure Victims.” Defense One, July 25, 2019. www.defenseone.com/technology/2019/07/russian-hackers-build-fake-skye-signal-pornhub-apps-lure-victims/158713/.

Turley, William S. *The Second Indochina War: A Concise Political and Military History*. Lanham, MD: Rowman & Littlefield, 2009.

UCDP. “Ukraine.” Accessed May 11, 2020. https://ucdp.uu.se/country/369.

Uppsala Universitet. “About UCDP.” Accessed May 3, 2020. www.pcr.uu.se/research/ucdp/about-ucdp/.

U.S. Army Recruiting Command. “Army Recruiting Discredits Military Draft Texts.” January 7, 2020. recruiting.army.mil/News/Article-Display/Article/2051787/urgent-news-army-recruiting-discredits-military-draft-texts/fbclid/IwAR22vIOsbx0KNcnZ-p0Igu0bIx2-GcBCjACJ2clbbLA9IPYBIEde_9_oduM/

Van de Weghe, Tom. “Six Lessons from My Deepfake Research at Stanford.” Medium, June 7, 2019. medium.com/jsk-class-of-2019/six-lessons-from-my-deepfake-research-at-stanford-1666594a8e50.

Voice of America. “Sinister Text Messages Reveal High-Tech Front in Ukraine War.” May 11, 2017. www.voanews.com/europe/sinister-text-messages-reveal-high-tech-front-ukraine-war.

Waked, Ali. “Hamas Sends Text Messages to Israeli Cell Phones.” Ynetnews, June 14, 2011. www.ynetnews.com/articles/0,7340,L-3648799,00.html.

# INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California