REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
23-04-2020	Master of Military Studies (MMS) thesis	AY 2019-2020

4. TITLE AND SUBTITLE
'I Agree': How 21st Century Big Data is Revolutionizing Military Capabilities in Phase 0

5a. CONTRACT NUMBER
N/A

5b. GRANT NUMBER
N/A

5c. PROGRAM ELEMENT NUMBER
N/A

6. AUTHOR(S)
Dugan, Sean W., (Captain, USA)

5d. PROJECT NUMBER
N/A

5e. TASK NUMBER
N/A

5f. WORK UNIT NUMBER
N/A

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
USMC Command and Staff College
Marine Corps University
2076 South Street
Quantico, VA 22134-5068

8. PERFORMING ORGANIZATION REPORT NUMBER
N/A

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

10. SPONSOR/MONITOR'S ACRONYM(S)
Matthew J. Flynn, Ph.D.

11. SPONSOR/MONITOR'S REPORT NUMBER(S)
N/A

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release, distribution unlimited.

13. SUPPLEMENTARY NOTES

14. ABSTRACT

Emerging technologies and commercial data markets provide novel resources for US cyber operations (CO) by generating Publicly Available Information and, or, Commercially Available Information (PAI/CAI). PAI/CAI fundamentally change the intelligence collection paradigm by allowing for passive, low risk Cyber Information Collection methods. The DOD should systematically use PAI/CAI within a prescribed model to enable Cyber Information Collection Operations (CICO) during Joint Force Phase 0 operations. Doing so would make the Joint Force more competitive with Great Power Competition (GPC) adversaries in the contemporary operational environment. Emerging hybrid warfare models and gray zone conflict within those models favor competitors who leverage PAI/CAI in lieu of information from state conducted intelligence collection operations. This research proposes the Joint Data Collection Efficient Frontier (JDCEF) model as a way for DOD CICO to leverage PAI/CAI while balancing CO operational risk and scalability.

15. SUBJECT TERMS
Cyberspace; Cyber; Advanced Persistent Threat; APT; Cyberspace Operations; CO; Publicly Available Information; PAI; Commercially Available Information; CAI; Cyberspace Information Collection; Cyberspace Information Collection Operations; CICO; C-ISR; C-OPE; Phase 0; Great Power Competition; Hybrid Warfare; Gray Zone; Irregular Warfare; Efficient Frontier

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			USMC Command and Staff College
Unclass	Unclass	Unclass	UU	51	19b. TELEPHONE NUMBER *(Include area code)* (703) 784-3330 (Admin Office)

United States Marine Corps

Command and Staff College
Marine Corps University
2076 South Street
Marine Corps Combat Development Command
Quantico, Virginia 22134-5068

MASTER OF MILITARY STUDIES

TITLE: 'I Agree': How 21st Century Big Data is Revolutionizing Military Capabilities in Phase 0

SUBMITTED IN PARTIAL FULFILLMENT
OF THE REQUIREMENTS FOR THE DEGREE OF
MASTER OF MILITARY STUDIES

AUTHOR: Captain Sean W. Dugan, USA

AY 2019-20

Mentor and Oral Defense Committee Member:	Matthew J. Flynn, Ph.D.
Approved:	
Date:	20200423
Oral Defense Committee Member:	Jill Goldenziel, J.D., Ph.D.
Approved:	
Date:	20200423
Oral Defense Committee Member:	Brandon Valeriano, Ph.D.
Approved:	
Date:	20200423

DISCLAIMER

Table of Contents

Page

DISCLAIMER i

TABLE OF CONTENTS ii

LIST OF ILLUSTRATIONS iii

EXSUM iv

PREFACE v

REPORT DOCUMENTATION PAGE vi

(1) INTRODUCTION 1
- (1.1) Hybrid Warfare and Gray Zone Conflict in Cyberspace 1
- (1.2) Cyber Strategy: Cyber Information Collection Operations 3
- (1.3) Research Question and Framework 7
- (1.4) Research Scope 8

(2) HYBRID CONFLICT 10
- (2.1) DOD Doctrine 10
- (2.2) Risk Analysis 11
- (2.3) Joint Force Operational Phases 14

(3) THE INTELLIGENCE PARADIGM 15
- (3.1) Joint Intelligence Preparation of the Environment (JIPOE) 15
- (3.2) Sensor Proliferation 17
- (3.3) Data Collection Authorities 22

(4) NOVEL DATA COLLECTION METHODS 30
- (4.1) Framework and Requirements for Implementation 30
- (4.2) Data Acquisition via Open Market 35
- (4.3) Data Acquisition via Data Brokers and Open Source Intelligence (OSINT) 39
- (4.4) Data Acquisition via Public Private Partnership 43
- (4.5) Data Acquisition via DOD Cyber Operations (CO) 45

(5) CONCLUSION 48

GLOSSARY 61

BIBLIOGRAPHY 64

Illustrations

Page

Figure 1. Cyberspace Information Collections 5

Figure 2. A proposed Cyberspace Information Collection Operations (CICO) Cycle 6

Figure 3. The Joint Data Collection Efficient Frontier (JDCEF).....32

Executive Summary

Title: 'I Agree': How 21st Century Big Data is Revolutionizing Military Capabilities in Phase 0.

Author: Captain Sean Dugan, United States Army

Thesis: Emerging technologies and commercial data markets provide novel resources for US cyber operations (CO) by generating Publically Available Information and, or, Commercially Available Information (PAI/CAI). PAI/CAI fundamentally changes the intelligence collection paradigm by allowing for passive, low risk Cyber Information Collection methods. The DOD should systematically use PAI/CAI within a prescribed model to enable Cyber Information Collection Operations (CICO) during Joint Force Phase 0 operations. Doing so would make the Joint Force more competitive with Great Power Competition (GPC) adversaries in the contemporary operational environment.

Discussion: The US DOD's leverage of novel information sources as potential intelligence information has not kept pace with the rapidly evolving cyberspace operational domain. This is partly because cyberspace operational doctrine and legal authorities are often years behind commercial industry innovations. This research examines ways to enable Cyberspace Information Collection Operations (CICO) through the Joint Data Collection Efficient Frontier (JDCEF), an intelligence collection model adapted from modern economic theory. This model would enhance intelligence collection against advanced persistent cyber threats (APT) who are expected to predominate 'new normal' hybrid warfare environments. This research addresses the legal basis for the JDCEF model in addition to ways for the DOD to acquire PAI/CAI during Joint Force Phase 0 operations and why the DOD should use this information to increase return on investment for CICO: Cyber Operational Preparation of the Environment (C-OPE) and Cyber Intelligence Surveillance and Reconnaissance (C-ISR). By wittingly or unwittingly co-opting private industry, the DOD can initiate and continuously conduct CICO in a completely passive and low risk manner. Moreover, the commercial and private sector set the strategic landscape of the cyberspace domain and, therefore, any type of cyberspace forward defense begins with PAI/CAI, not data directly collected by the DOD.

Conclusion: The DOD's systematic use of PAI/CAI is required to remain competitive among GPC adversaries of the contemporary operational environment. Emerging hybrid warfare models and gray zone conflict within those models favor competitors who leverage PAI/CAI in lieu of information from state conducted intelligence collection operations. The proposed JDCEF model provides a way for DOD CICO to leverage PAI/CAI while balancing operational risk and scalability with intelligence gain and the precision required to achieve CO effects. There is legal basis for DOD's use of PAI/CAI within current United States Code. Finally, the JDCEF model offers a more codified method for gaining indications and warnings of hostile APT group activity than the ad-hoc approaches currently employed by DOD entities.

Preface

I began this research to characterize how cyberspace operations fit into modern warfare concepts such as hybrid warfare, irregular warfare, the gray zone, and great power competition contact layers. Cyberspace, as an operational domain, is poorly understood, even less so in the context of modern warfare and great power competition. United States' great power competition adversaries leverage a variety of ends, ways, and means to exploit cyberspace asymmetric advantages while competing with the United States on the world stage. Paradoxically, the private sector is both enabling this exploitation and creating normative practices which make it harder to occur. I hope to challenge existing perceptions of the scale to which the Joint Force should consider cyber operations during Joint Intelligence Preparation of the Environment and, beyond that, propose a better framework with which to target Advanced Persistent Cyber threats attacking the United States on a daily basis.

I want to thank my wife, Charity, and three children for tolerating my weekday absences through my year of study at Marine Corps University. Without their support, this paper would not be. I would also like to acknowledge the considerable assistance I received from my primary research advisor and Marine Corps University Gray Scholar Program – Cyber lead, Dr. Matthew J. Flynn. Dr. Flynn's external engagement coordination and set-up of collaborative meetings with Dr. Brandon Valeriano and Dr. Benjamin Jensen expanded my horizons and exposed our cyber program group to the forefront of United States' cyber policy ideas with the authors of the 2020 Cyber Solarium Commission Report. Finally, Dr. Jill Goldenziel, my Lawfare elective professor, artfully adapted the elective to achieve economy of effort and time in support of research for this paper. I'm grateful for her willingness to merge course curriculum with student interests in the spirit of a more individually useful Joint Professional Military Education.

Report Documentation Page (SF 298)

1. INTRODUCTION

1.1 HYBRID WARFARE AND GRAY ZONE CONFLICT IN CYBERSPACE

The nature of cyberspace, as an operational domain, predisposes the United States towards a competitive disadvantage among its Great Power Competition (GPC) adversaries due to a US binary peace-war perception bias. This cognitive bias will become even more damaging to US interests as the hybrid nature of cyber operations (CO) and the gray zone environments in which they are conducted influence the US judiciary to restrict DOD CO on the basis of government overreach. Antiquated interpretations of domestic and international law continue to serve as legal precedents for opines restricting DOD's use of PAI/CAI to enable Cyber Information Collection Operations (CICO). This research examines ways to systematically conduct CICO through the Joint Data Collection Efficient Frontier (JDCEF), a novel intelligence collection model designed to enhance collection of technical cyber intelligence information against advanced persistent (cyber) threats (APT). The JDCEF incorporates PAI/CAI and other aspects of the contemporary intelligence paradigm to fundamentally answer two questions proposed for further study by CYBERCOM's 2018 Cyber Symposium. The first, "How does continuous engagement with adversaries change if DOD shifts from a war-focused mindset to a competition-focused mindset?" The second, "How do we (CYBERCOM) more effectively leverage intelligence and information to pursue our adversaries?"[1] CYBERCOM's 2018 Cyber Symposium proceedings identified two key requirements for fast and agile CO that were proposed in the form of the questions above. The Cyber Symposium is a day's long annual event showcasing CYBERCOM leaders and CYBERCOM's partners inside and outside government. The symposium discusses contemporary challenges for cyberspace operations and represents the leading edge of thought behind US cyber policy.

Understanding hybrid warfare and the gray zone are important for providing context that shows how both horizontal and vertical escalation within the cyberspace increase risk for US competitive disadvantage. Adversaries within the global operational environment increasingly provoke the United States with gray zone activities as the nature of GPC evolves in the 21st century.[2] Gray zone conflict itself may be viewed as adversarial and competitive but non-violent interactions at constant risk of violent escalation. In the event gray zone conflict does cross the violence threshold, kinetic action is often limited in scope and falls short of formal war. As common as gray zone activities are, the gray zone is not officially defined within DOD doctrine. US DOD doctrine even fails to formally define hybrid warfare, arguably a higher and more important concept within the contemporary GPC taxonomic hierarchy. These concepts are by no means ignored by the US military. As an institution, the DOD practiced limited hybrid warfare and some types of gray zone activities for decades, albeit in a de-facto and isolated manner using Special Operations Forces. However, the conspicuous absence of formal definitions for hybrid warfare and gray zone conflict is indicative of broader deficiencies in US strategic culture. The DOD will have difficulty countering future GPC hybrid warfare and gray zone activities without first formally defining the concepts. Indeed, military scholars recognized the inadequacy of the US ability to compete at thresholds below formal war and against multi-dimensional threats as early as 1996, suggesting that revisionist powers would exploit the US binary perception bias for asymmetric advantage in the gray zone.[3]

Anecdotal examples of suspected offensive cyber operations (OCO), such as the 2010 Stuxnet Worm[4] and the 2012 Shamoon Virus[5], may indicate nation state actors have strategic incentive in maintaining an ambiguous status quo for international cyber law. Legal ambiguity theoretically creates maneuver room under the guise of both ostensible legal legitimacy and

normative behavior. State actors would have less incentive to conduct OCO if international law more precisely defined them. Attribution confidence notwithstanding, nation-states use a shield of ambiguity for protection against activity characterizations which might be defined as OCO instead of espionage, a more internationally accepted nation-state normative behavior. Wide-spread legal consensus on international law as it applies to cyberspace suggests international law is deficient at defining OCO. NATO Cooperative Cyber Defence Centre of Excellence (CCD COE) analysis in the *Tallinn Manual*[6] and associated Tallinn Papers identified scarce cyber-specific treaty law, a near complete absence of cyber-specific customary law, and a consequent reliance on the cyber context interpretation of general international law to determine lawfulness of cyberspace activities.[7] The authors further stated that "…any interpretive endeavor is plagued with uncertainty and ambiguity, especially when engaged in with respect to novel activities such as cyber operations. This lack of legal normative clarity invites states to take differing interpretive positions… Controversy and inexactitude will surely characterize this process, which will be neither linear nor logical."[8] Similar and independent analysis of the *Tallinn Manual 2.0*, published more recently in 2017 and researched by nineteen international law experts, concluded that US OCO in response to economic cyber intrusions may only avoid breaching international law if (OCO) technical effects are (proportional) to the economic intrusions themselves and, or, the OCO are transient in nature.[9] In this instance, the *Tallinn Manual* authors drew distinctions between cyber economic intrusions and state executed OCO meant to counter them. However, target and effects based CO characterization may prove problematic at enabling future normative legal standards. The CO target, effect, or attributed party should not matter in so far as the CO technical activity itself. In this regard, the civilian sector has led the way in regulating CO by creating de facto international law through cyberspace interoperability standards. Technical

protocols established by companies like Cisco and Microsoft determine user access authorizations. Security encryptions associated with protocol access controls provide identifiable digital barriers, the breach of which constitute unauthorized access violations. Violations of this sort are a basis for claims in US legal courts.[10] However, these claims will do little to discourage illegal international cyber activity due to inadequate international formal legal standards for what constitutes cybercrime and the penalties for committing it.

Immature international law, or cyber context interpretations thereof, allows state actors a variety of legal justifications for OCO in a non-normalized environment. Acceptable international normative behaviors are established over time, in part, by effective legal standards. Inadequate international legal standards provide implicit incentive for GPC adversaries to exploit asymmetric advantages by conducting OCO within cyberspace. States less constrained by international norms will seek to negate their physical operational domain disadvantages through cyberspace activities. Quantitative analysis of OCO over time indicates that (likely) state sponsored malicious activity within the domain is increasing; this may be evidence supporting an inverse relationship between high legal normative standard environments and state sponsored OCO activity.[11] Whether the apparent OCO uptick is due to better awareness and detection ability or OCO horizontal escalation is the subject of scholarly debate. "Researchers analyzing the scope and scale of global cyber conflict face significant data collection challenges. In particular, the process of determining who is responsible for observed cyber incidents that are often covert by design produces research constraints for researchers seeking to describe modern competition, conflict and confrontation empirically."[12]

1.2 CYBER STRATEGY: (CICO)

The US has a myriad of interrelated options to counter malicious cyber activity amongst US diplomatic, information, military, and economic (DIME) components of national power. Discussing all of these is beyond the purview of this analysis. Essential to any option, however, is the ability to anticipate, detect, monitor, and respond to hostile cyber activities. The US can meet the first three of these requirements and enable the fourth by coordinated DOD, CIA, FBI, and DHS interagency Cyberspace Information Collection Operations (CICO)[13]. These operations, characterized by the following descriptions, should theoretically provide decision space to US cybersecurity personnel by yielding information which enables defensive cyber operations (DCO) or OCO in the form of Computer Network Exploitation (CNE).

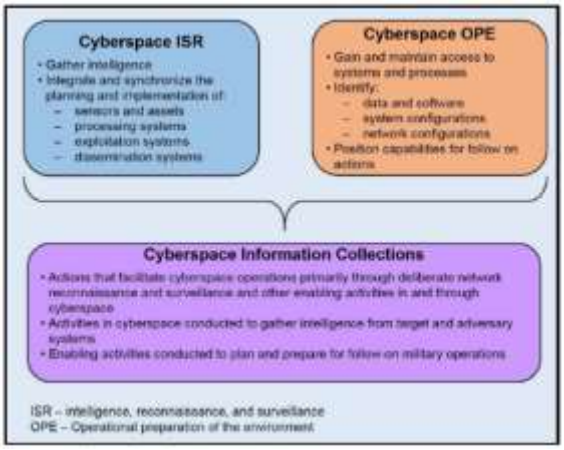

Figure 1: Cyberspace Information Collections, United States Army War College Center for Strategic Leadership, Strategic Cyberspace Operations Guide, (Washington, DC: Headquarters US Army, June 1, 2016), 18.

- Actions that facilitate cyberspace operations primarily through deliberate network reconnaissance and surveillance and other enabling activities in and through cyberspace.
- Activities in cyberspace conducted to gather intelligence from target and adversary systems.
- Enabling activities conducted to plan and prepare for follow-on military operations.[14]

Events such as the 2013 US Office of Personnel Management (OPM) indicate that coordinated interagency US CICO are deficient. In the OPM hack, the organization's databases were breached continually over a twenty-four month period by at least two likely related and Chinese affiliated entities.[15] OPM received no prior indications and warnings. OPM also responded to the attack in a manner which exacerbated its effects by failing to mount appropriate

DCO and not alerting the Department of Justice (DOJ) and DOD in a manner which mobilized elements of the Cyber National Mission Force (CNMF). This is a superlative example because the victim, OPM, is not a private corporation with little legal obligation to report or share threat information with the US Government. OPM is a federal government agency, the breach of which should have prompted an interagency response under the Director of National Intelligence (DNI) involving the seventeen members of the US intelligence community, including community member parent organizations such as the DOD, DOJ, Department of Homeland Security (DHS), and the Central Intelligence Agency (CIA). The notion that there was no coordinated interagency response provides some insight as to why attribution was so difficult. Beyond obvious considerations like insufficient OPM interagency communication and coordination, the answer lies in the often neglected CO category CNE, which exist in the space between OCO Computer Network Attack (CNA) and DCO Computer Network Defense (CND). CNE bridge the operational gap between OCO and DCO within an OCO/DCO-CICO cycle (see Figure 2). In the OPM hack, CNE should have been employed to enhance attacker attribution and enumerate attacker network vulnerabilities for potential Cyber National Mission Force (CNMF) OCO responses. The problem with US DOD cyber doctrine, however, is that CNE is underutilized within CO and, therefore, is infrequently enabled through multi-domain intelligence collection outside CO. Rather, CNE and activities enabling it should be a

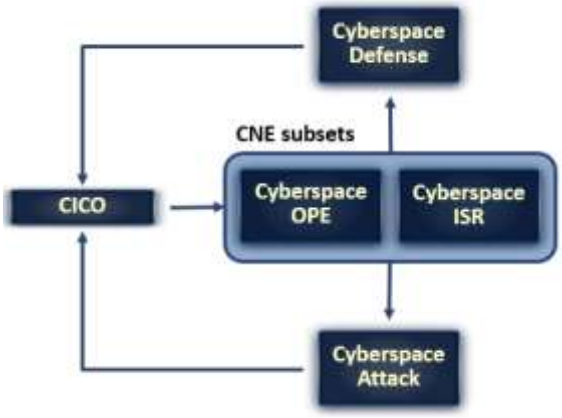

Figure 2: A proposed CICO Cycle (Adapted from Headquarters Department of Defense, Cyberspace Operations, Joint Publication 3-12 (Washington, DC: Headquarters Department of Defense, June 08, 2018), IV-5, C-1, GL-4)

foundational pillar of US cyber strategy writ large. Both OCO and DCO start with the intelligence and access CICO and CNE provide.

DOD cyber doctrine and legal authorities currently provide insufficient guidance and legal maneuver room for CNE. However, DOD policy and strategy are pushing doctrine to close the gap. The 2018 DOD Cyber Strategy advances defending forward and persistent engagement as two key concepts from the 2018 Cyber Command (CYBERCOM) Commander's Vision. In the CYBERCOM Commander's Vision document, the US CYBERCOM Commander stresses that "…the (US) must increase resiliency, defend forward as close as possible to the origin of adversary activity, and persistently contest malicious cyberspace actors to generate continuous tactical, operational, and strategic advantage."[16] The 2018 DOD Cyber Strategy states, "We will conduct cyberspace operations to collect intelligence and prepare military cyber capabilities to be used in the event of crisis or conflict. We will defend forward to disrupt or halt malicious cyber activity at its source, including activity that falls below the level of armed conflict…. The Joint Force will employ offensive cyber capabilities and innovative concepts that allow for the use of cyberspace operations across the full spectrum of conflict."[17] Defend forward, persistently contest, employ CO to collect intelligence, and the employment of innovative cyber concepts all signal a change in policy with profound implications for Cyberspace Information Collection operations.

1.3 RESEARCH QUESTIONS AND FRAMEWORK

Hybrid warfare and gray zone conflict legal implications seem most apt for deciding how to exploit the new reality of CICO. This research answers two questions in that regard:

- How does continuous (persistent) engagement with adversaries change if DOD shifts from a war-focused mindset to a competition-focused mindset?
- How does the DOD more effectively leverage PAI/CAI to pursue adversaries?

Answers to these questions are proposed through the systematic execution of CICO via the JDCEF cyber intelligence collection model. The research examines a legal and operational viability basis for each of the JDCEF's four echelons: open market, data brokers, public private partnerships, DOD executed CO. The model itself is designed as a more comprehensive framework with which to approach technical cyber intelligence information collection against cyber APT groups. Specifically, emerging technologies and commercial data markets provide novel opportunities to advance US CO through leveraging PAI/CAI during Joint Force Phase 0 CICO; the DOD should use PAI/CAI to enable CICO. A shift from war-focused to competition-focused mindsets is explored by examining PAI/CAI as a form of passive Open Source Intelligence (OSINT) collection which provides a low cost and low risk method for the United States to compete in the gray zone.

The research questions will be answered by first addressing how low risk CICO fit into hybrid warfare models that leverage gray zone competition as a primary method of engagement. A literature review establishes consensus as to the current state PAI/CAI as a source of technical data for intelligence information within the current Joint Force intelligence paradigm. The literature reviews allow for qualitative categorization of PAI/CAI sources as they apply to United States Code (USC) sections Title 18 Crimes and Criminal Procedure and Title 50 War and National Defense. Within these categories, precedent analysis and categorization frame current PAI/CAI collection methods. Finally, novel PAI/CAI methods are examined within the context of current legal and US cyber doctrine constructs.

1.4 RESEARCH SCOPE

Cyberspace, as an operational domain, is predominated by a few general types of activities: information operations (IO); intelligence collection (espionage); and offensive or defensive

operations which produce some type of logical or physical layer effect, even to the extent of damaging digitally controlled physical equipment such as with the 2012 Stuxnet worm. The scope of this research and analysis covers CICO and related enabling activities which drive further multi-domain intelligence collection. This paper will not cover what is commonly considered to be OSINT by contemporary intelligence collectors or analysts. Scraping publicly displayed information such as that posted on social media platforms is a commonplace means of exploiting PAI of the cyber persona layer.[18] In the context of this analysis, corporations like Twitter and Facebook function as forums which make this type of data available and a variety of DOD organizations have missions to exploit this after careful evaluation and screening to ensure that exploitation meets legal requirements.

This study proposes novel methods for collecting technical intelligence data through a variety of indirect means. These means are categorized as crowd sourcing, third party data brokers and, or, private-public-partnerships (PPP). Unlike cyber persona layer data, this data is not currently systematically evaluated and exploited by the DOD in a manner prescribed DOD doctrine. Data collected via crowd sourcing, third party data brokers, and PPP means would augment DOD intelligence operations, providing some of the same information as Joint Force Phase 0 intelligence operations. Joint Force Phase 0 intelligence operations are the primary source of information collection and intelligence production during Preparation of the Environment (PE).[19] The following doctrinal definition of information collection provides context for what PE intelligence operations are:

> Information collection is an activity that synchronizes and integrates the planning and employment of sensors and assets as well as the processing, exploitation, and dissemination systems in direct support of current and future operations (FM 3-55). FM 3-55 describes an information collection capability as any human or automated sensor, asset, or processing, exploitation, and dissemination (PED) system that can be directed to collect information that enables better decision making, expands understanding of the

> operational environment, and supports warfighting functions in decisive action. The intelligence warfighting function's contribution to information collection is intelligence operations.[20]

The FM 3-55 definition frames how CICO should support PE activities. The intelligence warfighting function's intelligence operations are a critical PE activity and expand the DOD's understanding of the operational environment prior to decisive action. In the context of the FM 3-55 definition, crowd sourcing and automated data brokers are an automated sensor information collection capability. Further along the CICO spectrum, PPP and DOD CO are intelligence operations.

2 HYBRID CONFLICT

2.1 DOD DOCTRINE

Understanding how DOD doctrine addresses the concept of hybrid warfare and the differences between Global Operating Model layers[21] of National Defense strategy is important for framing how and where the DOD should conduct CICO. US GPC adversaries employ hybrid warfare tactics to exploit asymmetric advantages while attempting to keep GPC below the level of armed conflict, or, at least within gray zone contact layers. Military and security studies scholars posit that hybrid warfare includes traditional warfare, irregular warfare (IW), terrorism, and criminal activities.[22] This is a problem for US national policy and national security strategy because IW is used as a de-facto hybrid warfare synonym in US doctrine. Conflating the terms causes ambiguity and poor synchronization among DOD elements charged with executing a synchronized IW strategy. Despite hybrid warfare's conspicuous absence in US doctrine, DOD IW publications acknowledge that,

> Compartmentalized distinctions of warfare rarely exist in practice…forces may well employ some combination of conventional and irregular methods.[23]
> With the increasingly rare case of formally declared war, traditional warfare typically involves force-on-force military operations in which adversaries employ a variety of conventional forces and special operations forces (SOF) against each

> other in all physical domains as well as the information environment (which includes cyberspace).[24]

Consider the Peoples' Republic of China (PRC) financial subsidization of Huawei Corporation as a form of hybrid or irregular warfare. PRC state subsidies provide Huawei competitive advantage over Huawei's international rivals, allowing Huawei to gain international market share through lower telecommunication infrastructure product price points. Instead of People's Liberation Army operations actively targeting foreign made digital infrastructure using CO, the PRC need only request the desired effect from Huawei's chief information officer. Further, it's also important to draw distinction between hybrid warfare and GPC activities in the gray zone. Critics might contend that, by definition, only armed conflict in hybrid warfare must be subject to the Law of Armed Conflict (LOAC). This interpretation fails to consider gray zone scenarios like the Huawei example in which states achieve military objectives through nonmilitary means. Theoretically, PRC could disable the Huawei telecommunications infrastructure of a target country with digital bombs rather than kinetic ones prior to military action. In the Huawei superlative, PRC achieves cyber domain superiority through state backed commercial industry dominance. As US DOD doctrine might phrase it, PRC could achieve its military objectives without ever escalating beyond Joint Force Operational Phase 0.

Few DOD institutional or doctrinal publications specify how CO fit into gray zone competition; this omission advantages US GPC adversaries who more effectively exploit cyberspace asymmetric advantage in hybrid warfare. Perhaps more worrisome, is how US gray zone activities, at least anecdotally, seem entirely relegated to the Military component of DIMEFIL. Though this research is less about hybrid warfare and gray zone conflict than it is about cyberspace intelligence collection, it is vitally important to understand that effective CICO must fully leverage gray zone ambiguity within the contact layer to negate asymmetric

advantages currently exploited by US GPC adversaries. Failing to effectively compete in the gray zone cedes and important part of the cyber domain.

2.2 RISK ANALYSIS

Empirical analysis of conflict from 1500 to 2015 indicates wars between great powers is at a historical low following a downward trend which began in the late 16th century.[25] Scholars posit a variety of historical forces for this downward trend. Invariably, the idea of limiting war, and therefore limited war, is historians' foremost consideration. Clausewitz, for example, called for an absolute war, but recognized that civilian realities will prevent this end from occurring. The advent of nuclear weapons introduced the prospect of absolute war, even the eradication of humanity, but again limits took hold. Given this historical arch, the evolution of war leaves that event limited no matter the time period. Cyber realities also confront this dynamic, reinforcing more than upsetting the means of limited war i.e. gray zone.

Other academic disciplines offer other means of assessment. The modern nation-state construct, (liberalism) international relations theory, feminization, cosmopolitanism, and an increased ability to reason are among the more innovative of those proposed forces.[26] Other scholars summarize theories with the notion that late modern era concepts such as Erich Von Ludendorf's *Der Totale Krieg (Total War)* or earlier modern era concepts such as Carl Von Clauswitz's *Absoluter Krieg (Absolute War)* have made warfare between major powers prohibitively costly and subsequently rare, largely due to civilian intervention to limit those costs.[27] The idea that nation-states of increasing populations have to continue competing among each other for limited global resources seems to suggest the latter theories are more accurate. In either case, it is logical to assume that competition has not disappeared. Rather, most competition evolved into hybrid warfare models where it occurs primarily below the level of

armed conflict and, or, as low intensity conflicts of limited scope and duration. This gray zone competition, as it were, advantages the United States but not for long. Democracy and free market economics synergistically set conditions for the birth of cyberspace but the domain is at risk of autocratic seizure. This is, in a way, a measure of American success, a validation of the American system and how the United States succeeded in pushing conflict into non-kinetic arenas. That the PRC, Russian Federation, Islamic Republic of Iran, and Democratic Peoples' Republic of North (DPRK) challenge American interests in cyberspace is a global win for non-escalatory conflict. However, it is also indicative of GPC gravitation towards low cost, low risk models.

Senior military leaders publicly state that hybrid warfare is a low risk, low cost activity which provides adversaries the opportunity to obfuscate their activities, throwing doubt on who is responsible for malign gray zone actions.[28] Alternatively put, hybrid warfare is a competition model which incorporates low-risk ways to achieve political objectives without necessarily provoking GPC adversaries into armed conflict. Great powers threatening the US favor hybrid conflict for this reason. Cyberspace too emerges as an increasingly utilized operational domain. CO and their inherent qualities such as attribution-deterrence dilemmas, potential for non-kinetic means to achieve effects, and geographic independence, among others, combine to rank cyberspace operations as the preferred hybrid warfare option among great powers. Of course, there are no available quantitative data sets contrasting cyberspace activities with those of other domains to indicate which hybrid warfare methods great power adversaries prefer. The basis for this preference forms through qualitative observation of state-attributed cyber-attacks (CA) over time. For example, CA against US entities likely attributed to China have increased year over year since 2015.[29] Similarly, the US Director of National Intelligence reported a 300% increase

in countries with CA capabilities over the period from 2007 to 2017.[30] In this sense, CA data indicates that GPC adversaries are maximizing their hostile or competitive actions within the non-escalatory cyber domain.

When faced with collective judgement from intergovernmental organizations like the UN, nation-states are less likely to challenge the international relations status-quo in an overt or attributable manner. State avoidance of being publicly labeled as a revisionist power bent on disrupting the status quo seems evident, particularly when juxtaposed with economic analysis of international sanctions on countries like the Islamic Republic of Iran and DPRK. US Congressional Reports highlighting the negative impact of economic sanctions on Iran are routinely used as a basis for further sanctions as coercion tools.[31] It is logical then, to assume that nation-states have a clear incentives to keep competition, or conflict, within politically acceptable confines. These incentives, in addition to the emerging dominance of cyberspace as the preferred hybrid warfare operational domain, is noteworthy. Great powers will likely allocate an increasing amount of intelligence resources towards low-risk, innovative methods enabling CICO to remain competitive in the cyberspace. Similarly, these operations should dominate how the DOD Joint Force prioritizes Phase 0 operations and conducts JIPOE over the next ten to twenty years and possibly in perpetuity. If the DOD's purpose is deterrence and, failing that, keeping war or competition limited to non-kinetic gray zone activities, how the DOD leverages cyberspace realities must ensure this end.

2.3 JOINT FORCE OPERATIONAL PHASES

CICO play a critical role in shaping the operational environment during phase 0. Joint Force operational phases within the Joint Force Operational Model are: shape, deter, seize initiative, dominate, stabilize, and enable civil authority. These phases are not linear, but lateral in nature.

Each phase has a different priority and shares a larger percentage of resources as joint force operations progress.[32] Military planners commonly refer to 'shape' as Phase 0 because actions within the phase, at minimum, provide a deeper and common understanding of the OE. Phase 0 activities prepare the OE in advance to facilitate joint force access, should contingency operations be required.[33]

JP 3-12, Cyberspace Operations, clearly defines how cyberspace exploitation, and by extension CICO, should support Joint Force execution of PE in Phase 0.

> Cyberspace exploitation includes activities to gain intelligence and support operational preparation of the environment for current and future operations through actions such as gaining and maintaining access to networks, systems, and nodes of military value; maneuvering to positions of advantage; and positioning cyberspace capabilities to facilitate follow-on actions.[34]

JP 3-12 further specifics that:

> All-source intelligence support to CO utilizes the same intelligence process used by all other military operations, with unique attributes necessary for support of CO planning…The process includes:
>
> > (1) Planning and direction, to include identification of target vulnerabilities to enable continuous planning and direction of CI activities to protect against espionage, sabotage, and attacks against US citizens/facilities and continuously examining mission success criteria and associated metrics to assess the impact of CO and inform the commander's decisions.
> > (2) Collection sensors with access to information about cyberspace.[35]

Collectively, C-ISR, C-OPE, and CNE provide information on and access into enemy digital information systems. Information and access then later enable a variety of effects through CO or Information Operations. The DOD should fully leverage alternative passive and low risk information collection methods to conduct broader CICO. The changing intelligence paradigm of the contemporary operational environment provides insight into what possible alternative collection methods could be.

3 THE INTELLIGENCE PARADIGM

3.1 JOINT INTELLIGENCE PREPARATION OF THE ENVIRONMENT (JIPOE)

JP 2-0 defines the joint intelligence process as consisting of six interrelated intelligence operations categories, the second of which is collection.[36] Data collected through intelligence operations forms the basis of the JIPOE process by supporting intelligence analysis which better allows commanders to understand their operational environments and make informed command decisions. Categorical data sources span all of the collective intelligence disciplines including, human intelligence (HUMINT), signals intelligence (SIGINT), electronic intelligence (ELINT), geo-spatial intelligence (GEOINT), and open source intelligence (OSINT), to only name a few. The quantity and quality of data obtained is usually a function of OE permissiveness. As a generalization, less permissive OE's have a lower quantity of and less qualitatively important collected intelligence data than more permissive OEs, the reason being that non-permissive environments present greater risk dilemmas for intelligence collection sensors. In the event the quality of data obtained in non-permissive OE does exceed that of permissive environments, data obtained in the former environment usually costs more per unit to obtain and is consequently more valuable. The data itself is the real currency of GPC, the gold standard of which is information regarding an adversary's plans and intentions. Reliable predictive intelligence is akin to seeing the future, knowing an opponent's chess move before it is made, or better yet, before an opponent conceives the move.

Though these concepts may seem elementary to the intelligence professional, they are often lost in how Joint Doctrine and US national policy prepares for CO, particularly with regard to the variety of APT groups now threatening US national interests. These groups operate clandestinely and in non-permissive to semi-permissive environments. The principal challenge for modern day military intelligence practitioners targeting these groups is to obtain the largest amount of and highest quality data possible, with the least amount of risk, at the lowest resource

cost per data unit. Low risk and low cost methods which provide large amounts of qualitatively important intelligence data apply to cyberspace just as they do any other operational domain. However, contemporary cyberspace policy and doctrine fail to address this principle. For example, CYBERCOM's defending forward and persistent engagement concepts are unclear in specifying how CICO should support CO directed against APT actors. At a higher level, the US Director of National Intelligence does acknowledge the importance of cyber threat intelligence data and how that data should support cyber operations in the OE. The 2019 National Intelligence Strategy (NIS) states, "This abundance of data provides significant opportunities for the IC, including new avenues for collection and the potential for greater insight, but it also challenges the IC's ability to collect, process, evaluate, and analyze such enormous volumes of data quickly enough to provide relevant and useful insight to its customers."[37] The first of four NIS topical mission objectives, cyber threat intelligence, prioritizes intelligence collection against state and non-state actors engaged in malicious cyber activities. The NIS further specifies that cyber threat intelligence, "…includes information on cyber threat actor information systems, infrastructure, and data; and network characterization, or insight into the components, structures, use, and vulnerabilities of foreign cyber program information systems."[38] These collective cyber threat intelligence target categories are technical data usually derived through CICO. Obtaining that data ultimately enables surreptitious access to adversary cyber systems, thereby obtaining intelligence information required to enable both OCO and DCO. It is only natural then, that the most effective CICO draw from the most comprehensive and broadest sources of information available, principally PAI and CAI.

3.2 SENSOR PROLIFERATION

At the cyberspace physical layer, sophisticated multi-sensor personal devices in the form of smart phones, tablets, computers, and other Internet of Things (IoT) connected devices pervade society and saturate the contemporary operational environment at unprecedented levels. At the logical and user interface cyberspace layers, data tracking features engineered into user interface software enable comprehensive analysis of users' content and lifestyle habits. Ubiquitous sensors in the contemporary operational environment are quickly obviating the heretofore resource constrained employment of human or technical intelligence collection sensors as a historical limiting factor for intelligence collection operations. Within a given OE, intelligence practitioners could only deploy a limited amount of intelligence assets (sensors) while maintaining an appropriate balance between detection risk, deployment cost, and intelligence gain-loss. Collecting cyberspace technical data using both digital code and physical form factors also obeys this principle. Each digital sensor must be protected with a level of tradecraft or employed in a manner commensurate with aspects of the sensor's technical or operational value. Both traditional intelligence gain-loss calculations and the risk vs. marginal cost of data acquisition still apply. History is replete with examples of how intelligence collection degrades as a result of compromised collection methods or how international relations deteriorate when intelligence operations are exposed. PE intelligence operations have an even higher implicit risk for superpowers like the US whom the international community looks to establish normative behaviors. PE operations and intelligence activities are specifically designed to prepare environments for future operations. If adversaries differentiate PE intelligence collection from that of traditional espionage, a greater case can be made for pre-emptive action on behalf of the target country. This is particularly true in cyberspace because of the domain's nascent or non-existent normative standards.

The US intelligence enterprise and CYBERCOM must adapt to the GPC new normal, a state of competition where adversaries leverage hybrid warfare models favoring gray zone competition. Within these models there is increased demand for low-risk intelligence collection practices. Risk mitigation for traditional intelligence operations is typically achieved through a higher degree of operational control, technological sophistication, resource allocation, and political support. Intelligence agencies often take great care to conduct collection operations in a covert or clandestine manner. Less detectable or attributable operations not only afford better access into operational areas of interest and collect better data by virtue of this access, but also have a lower implicit chance of degrading international relations. Passive collection operations, or those which do not generate an observable signature, are the most favored among intelligence professionals because they have lower detection risk than active collection operations. Passive bias is prevalent in all intelligence disciplines, i.e., if the same data can be collected in a passive instead of an active (signature generating) manner, sensors collecting that data have a lower risk of discovery. Significant financial resources are dedicated to research and development of passive sensors for these reasons. High research and development cost coupled with technological sophistication barriers to entry have historically given state-backed intelligence agencies a monopoly on ISR asset employment, data collection, and intelligence production.

Globalization and technological advances in private industry and society since the 1990s have forever broken the data collection monopoly historically held by governments. Global commerce and the intercommunicative technologies enabling it also put private industry at the forefront of establishing security and protocol norms for the cybersecurity industry.[39] Within cyberspace physical layers, technically sophisticated multi-sensor devices are ubiquitous in government and private sectors of society. These sensors exist in the form of cellular smart

phones, Institute of Electrical and Electronics Engineers (IEEE) 802.11 (Wi-Fi) devices, IEEE 802.15 (Bluetooth) devices, and most importantly, the vast and incalculable amount of computers connected to layered interfaces among Open Systems Interconnection (OSI) or Transmission Control Protocol / Internet Protocol (TCP/IP) internet connectivity models. Even televisions now have multi-purpose radio frequency antennas, audio, and video sensors integrated into home local area networks (LAN). In a 2015 Federal Trade Commission complaint filed by the Electronic Privacy Information Center (EPIC) against Samsung Electronics, Ltd, EPIC provided substantiated evidence that when a Samsung Smart TV voice recognition feature is enabled, everything a user said in front of the Samsung Smart TV was (at the time) recorded and transmitted over the internet to a third party, regardless of whether the audio recording related to the provision of service.[40] More broadly, conservative estimates of global population smart phone saturation begin at 45.12% according to sources which aggregate data from the United Nations Population Division, World Health Organization, International Monetary Fund (IMF), and the World Bank.[41] IMF estimates of global smart phone sales reached 1.5 billion in 2016 or approximately one new phone for every fifth person on earth.[42] When considering aggregate numbers of all types of internet connected devices, well over half of the global population owns or has access to some sort of internet connected sensor and uses it on a routine basis. These sensors are also vertically integrated throughout industrial and commercial applications and have pervaded the lives of everyday consumers in industrialized states.

The sensors are technically sophisticated. In a progression timeline consistent with Moore's Law, the technical data collection capabilities using hardware components of the contemporary smart phone have exceed capabilities of the most advanced military

communications devices as late as the mid 2000's. Advanced Micro Devices released their first dual-core processor, the Athlon 64 X2 3800+ at 2.0GHz and 512KB L2 cache per core, on April 21, 2005.[43] This chip would have been among the most advanced hardware components available for inclusion in most military static SIGINT or EW collection systems of the time. Today and in a mobile form factor less than 1/20th the size of equipment the Athlon 64 X2 was designed for, the Apple I-Phone XR runs the hexa-core Apple A12 central processor at 2.49GHz and 8MB L2 cache per core.[44] Potential issues with this comparison lie in the fact that most central processing unit (CPU) and mobile microprocessor measurements do not directly correlate, in part because the two processors are designed for applications with differing power usage and heat dissipation characteristics. Short of a more technical relative capability comparison, the reader should accept the idea that the A12 is orders of magnitude more multi-functional, efficient, and faster (when it needs to be) than the Athlon 64 X2. Other hardware features of the I-Phone XR, one of the most common smartphones on the contemporary global market, include: antennas resonant in most cellular communication electromagnetic radio frequency bands (450MHz – 2.1GHz); WiFi and Bluetooth radio frequency bands (2.4GHz – 5GHz); Global Positioning System (GPS) and *Globalnaya Navigazionnaya Sputnikovaya Sistema* (Global Navigation Satellite System – GLONASS) bands (1150MHz – 1610MHz). The iPhone XR's camera detects light frequencies within the visible light range bordering infrared and ultraviolet (430–750 THz) ends of the light spectrum. The phone's microphone is capable of acoustic energy detection beyond the audible frequency range (20Hz-20kHz) of the human ear. Finally, the phone also has a barometer, three-axis gyro (compass), accelerometer, proximity sensor, and ambient light sensor.[45]

Applications of these ubiquitous sensors are fully realized with technology such as software-defined radio (SDR) and software-defined networking (SDN). In SDR, equipment component functions traditionally managed by hardware (signal mixers, filters, amplifiers, modulators/demodulators, detectors, etc.) are instead implemented by software on any operating system connected to a receiver.[46] Similarly, software-defined networking (SDN) enables dynamic function to cyberspace physical and logical layers. SDN programming uses modifiable digital code to regulate network function in place of hardware. This allows for improved network performance and dynamic configuration models. In effect, both SDR and SDN allow for more flexibility with regard to receiving signals using any given antenna or sending data packets over any given computer network, respectively. This flexibility is critical when considering the repurposing of a cellar phone antenna or computer network adapter for alternative forms of CICO. Technically sophisticated sensor proliferation has, in short, vastly expanded cyberspace over the last decade and connects cyberspace to physical domain sensors covering a far greater percentage of the earth. Direct access to these devices in the form of DOD CO or indirect access in the form of DOD purchased PAI/CAI will be important for future CICO. In the indirect access form, the digital technology and its corresponding use agreements pressure users into abdicating their right to privacy on a volunteer basis. Conversely, the same technology also empower consumers to use their devices for financial gain or to support their countries national interests. The DOD should take note, these sensors and their digital connections are the new frontier of the cyber domain.

3.3 DATA COLLECTION AUTHORITIES

The 2017 National Security Strategy asserts that authoritarian regimes are less concerned by the LOAC and other domestic civil liberties legal protections than democratic societies.

Consequently, these regimes have less internally imposed constraints with their hybrid warfare approaches.[47] Their less constrained approach presumably translates to foreign and domestic intelligence collection practices which provide authoritarian regimes a higher intelligence production return on investment due to fewer bureaucratic restrictions governing their intelligence collection activities. This creates a higher relative cost basis for the US government. Legal restrictions such as the US Privacy Act of 1974 and US Codes (USC) Titles 10, 18, and 50, yield substantial competitive advantage to GPC adversaries with respect to state-sponsored intelligence collection activities. GPC adversaries have always sought to exploit US legal compliance through the asymmetric use of state-sponsored intelligence collection activities and US adversaries may be finding new exploitation avenues through open PAI/CAI data exchange markets. The DOD and US government writ large must consider that open market purchase of information is not tantamount to collection to remain competitive in a contemporary gray zone intelligence paradigm. Failure to acknowledge this idea will further encourage US adversaries' adoption of hybrid warfare approaches which preclude the US ability to identify foreign surrogates, proxies, or other state backed criminals who hide behind the DOD's antiquated application of intelligence collection activities governed by EO 12333, The Privacy Act of 1974, and US Code. Lawfare scholar Orde Kittrie would describe this as compliance leverage disparity lawfare, "…a method designed to gain advantage from the greater influence that law exerts over an adversary."[48] Whereas the US Privacy Act of 1974 and Executive Order (EO) 12333 sensibly restrict the US Government from collecting or maintaining information on US citizens in the name of protecting Americans' civil liberties, these legal constructs fail to govern data products made available by commercial entities in open exchange markets. In this respect, GPC adversaries turn US respect for domestic law into a strategic vulnerability. Maj. Gen.

Charles Dunlap Jr. provides insight into this method as how, "US adversaries (see the United States') political culture's respect for the law as a 'center of gravity' to be exploited."[49] There may, however, be a PAI/CAI gray area within the US legal framework which allows the US government to compete with GPC adversaries on a more equitable basis.

The real questions posed by PAI/CAI legal analysis is, if the DOD purchases the same type of data which would otherwise be obtained through DOD collection operations, is the data purchased the same as data collected? Further is the data categorized according to its projected end use under FISA and USC Title 10 or Title 50 authorities? Should the interpretation be that, regardless of the data's projected end use, the DOD is free to use the data (means) for a variety of applications (ends) in whatever method (way) the DOD chooses? How does the data fit under current FISA laws and information collection, storage, and dissemination requirements?

Current DOD data collection authorities are unclear with regard to data collection via PAI/CAI, the majority of which is information consumers explicitly or implicitly consented to the sale or provision through end user agreements. In general, few US laws govern commercial data broker collection of PAI.[50] The Privacy Act of 1974, "Does not apply to data collected about persons outside the United States, nor does it protect the privacy records that are maintained by the private sector or local state governments."[51] Legal scholars and industry experts maintain that the protection of personal privacy, including the protection of personal data, is at best a patchwork of federal, state, constitutional, statutory, and case law.[52] With respect to federal statutory law, "…Congress has adopted a legislative approach which is sectoral in nature… (a) law-based means for protecting personal privacy in some areas, but not in others."[53] In a 2012 Federal Trade Commission (FTC) report titled *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Business and Policymakers*, the FTC

acknowledged that data brokers, most of which are excluded from the Fair Credit Report Act (FCRA), generally operate absent any formal legal restrictions regulating their data collection.[54] The US Senate came to a similar conclusion in 2013, concluding that (non-FCRA regulated) data brokers, "…operate with minimal transparency and are subject to virtually no statutory consumer protections."[55] This is significant in showing that federal law underregulates commercial PAI collection and fails to make it illegal.

The FTC and US Senate opine on the idea that there is scant legal basis restricting potential data use applications for the commercial data broker industry, which, by all estimates, continues to grow due to financial incentives underlying PAI collection. By 2012, the data broker industry had generated 150 billion dollars in revenue, an amount twice the size of the entire intelligence budget for the US Government that same year.[56] *Privacy's Blueprint*, by Woodrow Hartzog, believes that most companies rely on machinations of contract law by clicking "I agree to the Terms of Use" buttons as "consent" for privacy invasive practices which produce information "…extracted via sleight of hand under the auspices of a well-functioning market."[57] From the DOD's perspective, how an organization obtains free-will consent should not matter insofar as it was acquired to begin with. The US legal framework allows PAI to be sold in the form of CAI on an open market through a manner in which end users consent to their information commoditization. In this sense, the government is not directly collecting on US persons. The government is buying a product, a commodity. The DOD's use of data broker CAI products should not be subject to The Privacy Act of 1974 or its stipulations enforced through EO 12333. Plainly, these stipulations specify that direct collection of PAI by US Government Intelligence Community elements be conducted, "In accordance with procedures approved by the Attorney General, in consultation with the Director of National Intelligence, and in a manner

consistent with each element's specific authorities."[58] The Privacy Act provides US citizens rights and assurances by imposing obligations on the federal government when federal agencies collect, maintain, and use personal information considered to be part of a public system of records. EO 12333 further specifies that PAI must be collected with consent and by Intelligence Community entities with a valid mission requirement under specific retention and dissemination criteria. The DOD should not be put in a position questioning whether it can use the same commercially available databases which countries like PRC or Russia have open market access to. It is logical to assume US GPC adversaries are buying this information because current US data privacy laws do not require data brokers to disclose who their customers are.[59]

Much of the CAI sold by US domestic data brokers is not generally pursued by the DOD or other US intelligence agencies due to federal statutory concerns and, in many cases, the DOJ cannot collect or maintain access to the information without a court approved warrant. In other precedents more useful to the DOD, the DOJ and DHS purchase application generated marketing data, including geo-locational data, from data brokers and telecommunication providers.[60] The Department of Homeland Security Customs and Border Patrol 2018 Privacy Impact Assessment states,

> CBP may use commercially available location data acquired from a data provider in order to detect the presence of individuals in areas between Ports of Entry where such a presence is indicative of potential illicit or illegal activity. The goal is to utilize this data to detect the presence of – but not identify – individuals in an area which CBP has identified as an area of interest, consistent with CBP statutory authorities, federal law, and DHS policy. Data from such datasets is compiled by a third-party provider from multiple commercial sources and anonymized, offered for purchase, and can then be acquired by public or private entities, including CBP.[61]

This type of activity presumably falls under the purview of the Foreign Intelligence and Surveillance Act (FISA) of 1978, USA PATRIOT Act, Protect America Act of 2007, FISA Amendments Act (FAA) of 2008, and the USA Freedom Act of 2015.

The problem with both FISA and its subsequent amendments is that their language only addresses the federal government's direct execution of surveillance, collection, or acquisition of data on persons in protected categories. None of the FISA language pertains to information indirectly collected through CAI purchase. As if to further exacerbate FISAs authority gaps, the 1974 Privacy Act enables commercial data brokers despite its purpose being to protect US persons' data privacy. The act attempts to protect privacy through limiting the circumstances in which US persons' personally identifiable information (PII) is retained and shared[62] by the federal government in addition to providing US persons' partial control over their PII in relevant government databases.[63] However, the private sector is not beholden to the same standards as the federal government. The private sector conducts financially motivated corporate surveillance in a manner far more invasive than the government will ever be able to.[64] This is possible because the US consumer allows it through consent. Corporate surveillance practices generate broader questions about privacy and what type of information private corporations collect through engineered consent in addition to questions about how this information is being used. The true irony is that US GPC foreign adversaries have access to US commercial databases to which the US DOD does not because of conservative statutory opinions. Similarly, the DOJ only accesses information from these databases via court approved warrants.

Arguments countering the DOD's need for domestic PAI/CAI stress that there are no restrictions governing the DOD's purchase of non US entity information from foreign or domestic data brokers and that there is no need to purchase information which likely contains data on US entities. However, cyberspace technical norms of the contemporary global commons will seldom provide reasonable means with which to distinguish US persons and corporations from foreign ones within global data sets. Further complicating discernment is that some of this

data is provided directly by its original collectors such as telecommunication providers and other data is provided through secondary or tertiary PAI/CAI aggregators (data brokers). There is substantial federal regulation regarding data provided through original collectors such as telecommunication providers. The USA PATRIOT Act, along with its 2007 Protect America Act and 2008 FAA, account for the possibility of Americans' PII in global telecommunication data collected by federal government entities while simultaneously permitting the federal government to directly collect on sources of foreign intelligence information. The legislation enables federal organizations operating under USC Title 50, among other federal organizations, to surveil and collect global technical cyber information flowing through US digital infrastructure. This ability is critically important in an era of packet switched networks routing global communications through equipment owned by US telecommunication companies.[65] FAA sub-section 702b specifically empowered the US Attorney General and Director of National Intelligence to jointly authorize data collection targeting foreign entities with rules for determining the foreign nature of targets and regulating federal activity in a manner consistent with the Fourth Amendment of the United States Constitution.[66] However, FAA sub-section 702 powers only went so far. Public dissent in the wake of former NSA contractor Edward Snowden's illegal disclosures prompted national scrutiny of intelligence and surveillance laws, including FISA. This outcry resulted in a US 2nd Court of Appeals May 2015 ruling which stated that Section 215 of the Patriot Act did not permit something so broad as the NSA's bulk metadata (haystack) collection program. The 2015 USA Freedom Act later provided NSA access to the same metadata through court order; instead of NSA direct metadata acquisition, US telecommunication and internet service providers would be obligated to furnish metadata to the NSA through Foreign Intelligence Surveillance Court (FISC) order.[67] This provides the US

Federal Government reasonable legal access to consumer data that consumers do not consent to the sale of. However, US Federal law neglects rules for information made available via consumer consent, or information end users willingly and knowingly consent for sale to third parties under end user agreements.

Section 222 of the Federal Communications Act regulates data generated from original private sector collectors, such as telecommunication providers, and made available in open exchange markets.[68] This act requires providers to protect their customers' sensitive personal information, including location data. Legally, providers cannot simply sell their consumers' information to anyone willing to buy it. The difference between primary source data and CAI is best explained by how a user can often turn off their device settings which reveal their location to marketers or third parties but telecommunication providers need to know a phone's approximate location to provide wireless service.[69] However, data generated from primary source entities, the same data regulated by the 2015 USA Freedom Act, is increasingly blurred with other CAI. Federal Communications Commission filings as of February 2020 allege that CAI data aggregators used the data feeds from telecommunications primary source entities for illegal purposes. The FCC alleges these entities violated FCA Section 222 by disclosing real-time location data. Commercial data brokers do not fall under FCA Section 222. These brokers monetize all types of consumer data in the form of database commodities available for purchase. Those databases commodities include cyber technical information such as users' device models, operating configurations, historical connected LAN topographies, and locational data, among other types. Some data fields contain PII but many are minimized to exclude it.

DOD's use of PAI/CAI from domestic or foreign data brokers would not be contrary to the spirit and intent of the 1974 Privacy Act. In this sense, use of the data does not constitute

government overreach. The US government specifically created the act to mitigate federal intelligence collection abuse concerns and to restrict the federal government's use of information technology systems such as the modern internet to jeopardize citizens' privacy.[70] Federal regulatory guidelines could be made clearer to obviate the DOD's need for pre-purchase data screening prompted by concerns it contains Americans' PII. Purchases of databases which the DOD had reason to believe contained information on US persons could be made possible without prior intelligence oversight compliance evaluation under EO 12333. Benefits of wholesale acquisition in this manner are realized through the timely and substantive analysis of information. DOD purchasing entities would be free to purchase CAI products from any domestic or foreign data broker at any time for any reason, later evaluating whether use of specific information within the database could be retained pursuant to relevant legal and regulatory guidelines. Protecting American civil liberties should begin with more restrictive domestic US federal data privacy laws that regulate the type of data available on open exchange markets, not regulating what the government can buy on those markets. Regulating data collection at its source would eliminate the need for more cumbersome bureaucratic FISA legal filters because any products on the open market might be considered legally available via contract law consent. Regardless of whether federal data regulation happens at the collection source or at the CAI product purchase level, two things are clear. Data broker collection of PAI/CAI is legal and it is happening through consumer consent and device or software collection control designs.[71] Consider the ramifications if this argument is wrong. Imagine a scenario where the DOD cannot leverage data broker collected PAI/CAI but foreign intelligence services can. If critics claiming government overreach contend that the DOD cannot legally acquire and, or, retain PAI/CAI, then US federal consumer privacy and data protection laws inadvertently

create the largest counter intelligence threat in the history of the United States. Unbounded data aggregation and re-identification possibilities theoretically enable US GPC adversary precision targeting of US DOD and other federal personnel on an unprecedented scale by way of the cyber domain.

4 NOVEL DATA COLLECTION METHODS
4.1 FRAMEWORK AND REQUIREMENTS FOR IMPLEMENTATION

Earlier sections of this analysis established a compelling case for hybrid warfare gray zone competition as the new normal among low-risk GPC models. Within the hybrid warfare construct, cyberspace emerges as the preferred operational domain due to its implicit risk-benefit ratio. Various technical, legal, and geo-spatial advantages also give CO greater data collection potential, plausible deniability, and operational reach, respectively. Intelligence paradigm fundamentals also favor passive, low-risk collection methods in non-permissive environments. It is logical then, to infer that cyber operations will continue to increase in frequency and scale as GPC evolves within gray zone contact layers. At the GPC level, the PRC formally includes CO in its planning for future war, a consideration best revealed in *Three Warfares* and *Unrestricted Warfare* (超限战). The Russian Federation's use of the hybrid warfare concept and an emphasis on non-military methods as part of Russian Chief of General Staff Valeriy Gerasimov's active defense strategy favor cyber operations as a preferred way to achieve strategic objectives.[72] More than that, two decades worth of PRC and Russian Federation doctrine changes are examples of how GPC adversaries embrace lateral, instead of linear, thinking to conceive and adopt innovative solutions which leverage asymmetric advantages to accomplish military end states.

The DOD must develop a novel CICO framework to further enable US strategic cyberspace objectives, particularly within the defending forward and persistent engagement strategies proposed by the 2018 CYBERCOM Commander's Vision, 2018 National Cyber Strategy, and the 2018 National Defense Strategy. These policy documents are the foundation of future cyber doctrine. The persistent engagement and forward defense concepts they propose are themselves analogues of Gerasimov's proactive measures. The framework would be neither discrete in its partitions nor exclusive from other intelligence disciplines. Rather, employment of methods within the framework would overlap and could also be useful to SIGINT, IMINT, and ELINT collection, among other forms. The framework would be based on a synergy of economic principles and intelligence collection practices in addition to the legal basis of individual consent or even witting participation to some degree. The title of the framework might be something to the effect of the Joint Data Collection Efficient Frontier (JDCEF), an acknowledgement to the investing model proposed by Nobel Laureate Harry Markowitz in 1952. (see Figure 3) The

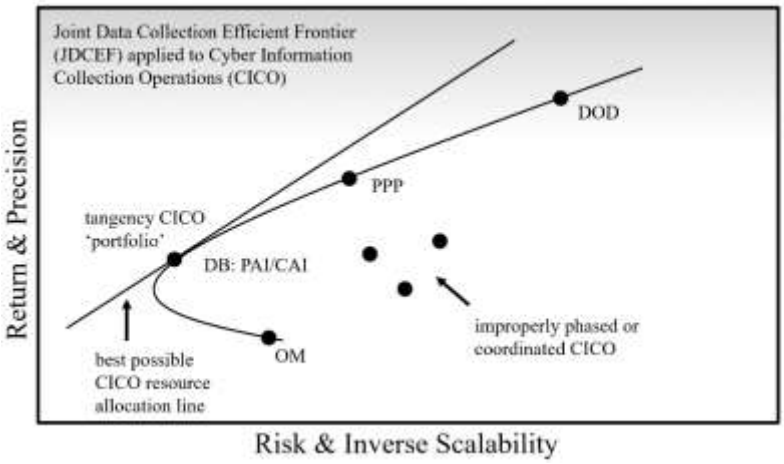

Figure 3: The Joint Data Collection Efficient Frontier (JDCEF)

efficient frontier is a set of investment portfolios that offer the highest expected return for a defined level of risk or, conversely, the lowest risk for an estimated level of expected return.[73]

The framework would fully leverage public-private-partnerships (PPP) on a collective (company) or individual private citizen level to exploit the eroding monopoly the US government traditionally maintained over intelligence data collection and analysis. The rise of

private corporations such as intelligence firms, defense security contractors, and commercial data brokers have already either deliberately or through multi-use product designs privatized vast segments of the national defense industry. For wealthier nations, these private corporations are often de-facto proxies for the states they represent.[74] Incorporating these companies into a formal framework would take little in the way of establishing new relationships as many PPPs already exist within the US defense industrial complex. The JDCEF framework might exist as broad echelons comprising four categories of data acquisition: open market (OM), data broker (DB), PPP (USG contractor), DOD CO. The categories overlap and exist on a scale characterized by operational precision on the Y-axis and operational scalability on the X-axis. The two variables, precision and scalability, are inversely proportional. Echelon subcategories may further divide the main data acquisition categories and may also be templated on the X-axis. Collectively, these distinctions would not be mutually exclusive. The same APT target can first be assessed through PAI/CAI available on the open market, refined through data broker information aggregation, further tracked through PPPs, and finally exploited through CYBERCOM executed CICO.

CICO within this model would naturally gravitate towards the most passive, non-invasive, and broad scope forms, particularly those forms which are legal through explicit host system user authorization. In the JDCEF framework, these forms exist within the open market where crowdsourcing is the superlative example. Crowdsourcing is colloquially defined as the utilization of the general public to complete a project, usually without compensation.[75] For the purpose of this analysis, crowdsourcing includes compensation as a financial incentive within various crowd sourcing models. As a means of intelligence collection, crowd sourcing

cyberspace or SIGINT technical data relies on a type of distributed collection principle to be valid.

Basis for distributed methods span a wide range of industries including data analysis, data storage, data brokerage (a combined form of collection and analysis), logistics, and land management, to name only a few. For distributed data analysis, the University of California Search for Extraterrestrial Intelligence (SETI) at Home program, known as SETI@home, is a method for academic researchers to send large amounts of radio telescope data to mainly personal computers across the world for data analysis. The many, many personal computers function as a virtual super computer which enables UC Berkley researchers to analyze far greater data than their own resources would allow. The program provides no financial incentive to participants and instead relies on their altruistic and ideological motivations to provide free computing power to complete the SETI@home program goals. Nevertheless, SETI@home is over twenty years old and has a total of 1.7 million total users.[76] It serves as one of the oldest proven models of crowdsourced data analysis in that it successfully and globally recruits individuals to allow their personal digital devices to analyze information in support of a secondary effort.

Cryptocurrency mining is a newer version of consumer distributed analysis which relies on the same technical principles as SETI@home but provides financial incentive to its participants. Cryptocurrency miners are private individuals or companies that provide use of their computers' processing power to analyze data. These entities are issued a certain number of cryptocurrency units of value in exchange for their computing power provided.[77] Some publicly available evidence substantiating the economic incentive for such systems projects the overall value of the cryptocurrency market to reach $1.4 billion US dollars by the year 2024.[78] The

significant of both SETI@home and the cryptocurrency market is plainly evident. People are willing to allow their personal devices to be used for secondary analytics. The same is true for information and collection on behalf on the US government, albeit on a smaller and less direct scale.

The US Government directly crowdsources data analysis, design, and collection through a variety of approaches. These include the Presidential Innovation Fellows Program and various citizen science programs in which individuals share and contribute to data monitoring and collection.[79] Indirectly, the US government routinely purchases information from data brokers and credit bureaus. In 2013 the US Treasury Department began using consumer credit bureau Equifax's 'The Work Number' database as part of a Treasury Department 'Do Not Pay Business Center' pilot program aimed at enhancing the department's ability to combat fraud and other improper government payments. The Work Number database contained 54 million active salary and employment records and 175 million historical records collected from more than 2,500 US employers.[80] DOD direct collection of the same information contained in The Work Number database would be prohibited under current EO 12333 intelligence oversight regulations and Title 10, 18, or 50 authorities. The worry here is that the DOD's or DOJ's routine and unwarranted use of the information would constitute government overreach and violate American civil liberties.

Direct versions of crowd sourcing via distributed data collection exist on a reactive basis within the cybersecurity industry itself. Private corporations regularly provide cyber threat intelligence information to the USG on a voluntary and informal basis. Entire organizations such as the Office of the Director of National Intelligence (ODNI) Cyber Threat Intelligence Integration Center (CTIIC) are dedicated to the aggregation and socialization of cyber threat

information across the USG and non-government (private) entities.[81] The primary shortcoming of this process lies in the unsystematic and convoluted manner in which it occurs. CTIIC itself lacks direct liaisons with the private sector. Instead, it works through other government agencies that do have liaison relationships and helps downgrade information and analysis those agencies have for sharing.[82] Well intended as they may be, these systems fail to realize a higher potential for synchronized government-private sector data collection potential because the systems do not provide financial incentive to private entities whose participation is ultimately non-compulsory.

4.2 DATA ACQUISITION VIA OPEN MARKET

The DOD, and US government writ large, would benefit by financially incentivizing crowd sourced technical cyber data collection through the use of contemporary data commoditization strategies. Strong economics research data indicates distributed intelligence collection via crowd sourcing would be both viable and, in the context of an efficient frontier model, incur the lowest risk by way of obtaining certain types of technical cyber intelligence data. In 2003, the Defense Advanced Research Projects Agency (DARPA) canceled a program which would have created a Policy Analysis Market allowing traders to negotiate various forms of geo-political risk.[83] The program aimed to investigate whether trading in geo-political futures contracts might accurately predict future geo-political events and discover how traders perceived connections between on-going events, thereby indirectly crowdsourcing various forms of OSINT analysis and intelligence collection related to the events in question. DARPA canceled the program due to critics' claims the program provided a system of "terrorism futures." However, the program's concept was sound and based on the concept of information aggregation, a relatively new form of financial market often known as a prediction market but which also goes by the name financial market or event futures.[84] While this analysis is not on prediction markets per say, these markets provide

sufficient basis for crowdsourcing cyber intelligence information and the utility of aggregating information from broad quantitative and qualitative sources of that information. The wisdom of crowds is alternatively expressed as the idea that assessing large groups of people yields results collectively more accurate than individual experts when it comes to problem-solving, decision making, innovating and predicting.[85] One key difference among crowdsourcing and prediction markets is that prediction markets rely on people betting on their beliefs about current or future events because they have a financial incentive to bet correctly on the future outcome, while other mechanisms like crowdsourcing do not exploit this.

Twenty first century sensor proliferation makes possible mechanisms which provide financial incentive for individuals or corporations to collect cyber information collection operational data and either wittingly or unwittingly provide that data to the USG. For example, a USG or defense contractor affiliated smart phone or personal computer application could be made commercially available and provided to the public. The USG could pay users of this application a fee which might vary based on the individual's pattern of life and access to certain geographic or virtual areas of interest. Application functions would vary by device but could generally perform functions like the automatic mapping of wide area network (WAN) connections using a variety of network mapping tools upon router or server connection. Other application functions might use SDR to repurpose the device's antennae for sensing 2-5th generation telecommunication carrier cellular network frequencies, 802.11, 802.15, and other wireless sensor networks (WSN) resonant with the antennae bandwidth but not necessarily utilized by the device antennae under native system configurations.[86] The application would also automatically run in the background of the user's device, continually mapping and sensing, requiring no action on behalf of the user. Payment might be based on the qualitative, type of

WAN, or quantitative, amount of local area networks (LAN), mapped in a given period of time or on a singular basis: WAN = $1; LAN = $.01. Even a fixed $5 payment might fund 8,800 users to each continuously run the program for a month, or 720 run-time hours. Total cost to the DOD in that scenario would be $44,000 or the publicly reported cost to operate an F-35 Joint Strike Fighter for one hour.[87] Crowdsourcing technical CICO via this method would advance US CO in a passive, non-escalatory manner.

The financial incentive yield curve and the technical possibilities of the software are potentially endless. The concept, however, remains the same. Foreign nationals across the world would be paid to passively run a background application on their smart phone or computer which would not collect the content of their personal communications but the wired and wireless electromagnetic information about the operational environment in which they live. This information would be funneled to NSA databases for evaluation and further analysis. Vast segments of the service sector would have implicit financial incentive use the software. Taxi and bus drivers, truck drivers, rail operators or other individuals with regular and widespread area access might be early adopters of the software. Recursive methods might even be used to provide a higher payment to individuals with better access to and pattern of life in areas of interest, further incentivizing their use of the software while they go about their regular activities.

Beyond the network mapping potential, the DOD provided software could make full use of an individuals' smart phone or personal computer sensors, using locational data to push the user notifications to take pictures of areas of interest within their pattern of life. Software camera modifications might be used to provide ground level spectral imagery of areas previously only accessible by advanced National Reconnaissance Organization assets.[88] Smart phone barometer, compass, accelerometer, and proximity sensor might be used to assess route

navigability and traffic patterns. This kind of extensive intelligence sweep would mean US intelligence operations would no longer waste time and assume operational risk in non-permissive areas by gathering basic PE intelligence information.

Critics of this method will counter with a variety of arguments: adversaries would become inadvertently sensitized to cyber or physical environment areas of interest which would compromise intelligence operational objectives, adversaries might spoof or falsify data with deception countermeasures, individuals would game the payment system and network multiple and nearly identical personally carried devices to receive higher payments (think of users carrying multiple devices to multiply their gain during the same geographic or digital trip). A variety of counter tampering technological measures could be used to ensure data integrity, secure certificates and end-to-end encryption come to the forefront as two obvious choices. Even beyond technical counter tampering measures, the economic analysis provided above indicates that, although tampering may happen, the data mean would be largely accurate. Mathematical analysis may support this assertion through the long-tail mean. Advocates of Chris Anderson's *Long Tail Effect* contend, "The long tail is a statistical pattern of distribution that occurs when a larger share of occurrences occur farther away from the center or head of distribution. This means that a long tail distribution includes many values that are far away from the mean value."[89] Throwing out the short tail or, likely tampered data, and then averaging the mean of the long tail, or the second mean, would likely provide an accurate value. Crowed sourced HUMINT collection methods proposed through power law and long-tailed distribution modeling suggest that many separate (one time source) HUMINT reports collected from larger relative populations exceed the value of the same quantitative amount of HUMINT reports collected from smaller relative populations.[90]

Finally, if decision makers think the decision politically unviable or technically unfeasible in the hands of foreign nationals, the program might be provided to government personnel in the following order determined by descending intelligence collection legal authorities: DOD or interagency personnel operating under USC Title 50 authorities, DOD electronic warfare (EW) personnel operating under USC Title 10 authorities, all DOD personnel operating under Title 10 authorities, all federally employed personnel. Restricting program distribution would limit OE saturation but still provide continuous persistent survey data for areas of active DOD operation.

4.3 DATA ACQUISITION VIA DATA BROKER AND OSINT (PAI/CAI)

The USG should co-opt existing commercial data brokers by sensitizing them to operational environment technical collection requirements via the federal government bidding process. The commercial data broker industry currently provides the most revealing example of distributed indirect data collection. Commercial data brokers are companies that collect, analyze, and package consumer sensitive and personal information and then sell it to other companies for a variety of purposes.[91] Consumer data collection is not new; companies have been gathering individuals' personal information for decades. Some industry experts date this systemic collection back to early consumer credit scores in the 1950s.[92] Though originally developed for the consumer credit industry, the data (information) brokerage industry has expanded to serve a wide variety of other industries, compiling information from an even wider variety of sources. These sources include:

- Retailers and merchants via Cooperative Databases; sales and customer lists
- Financial sector non-credit information (PayDay loan, etc.)
- Financial sector credit information (Equifax, Transunion, Experian, etc.)
- Multi-Channel direct response
- Survey data
- Catalog orders (phone and online)

- Warranty card or rebate registrations
- Social media interactions (dependent on data broker interactions/agreements)
- Loyalty card data (retailers)
- Public record information
- Medical records
- Web site interactions (via ISPs, search engines, internet browsing software, etc.)
- Lifestyle information (Fitness, health, wellness centers, etc.)
- Non-profit organizations' member or donor lists
- Subscriptions (online or offline content)[93]

Data broker individual dossiers begin with information referred to as personally identifiable information (PII) such as an individual's name, social security number, date of birth, telephone numbers, etc. The information dossiers then expand to include a wider variety of sensitive personal information (SPI). SPI includes information about individuals' demographic, employment history, court and public records, social media data, financial data, travel data, purchase history, real estate or vehicle ownership, professional licensures, legal judgements, court records, marriages, divorces, workers compensation claims, etc.[94] Even non-personally identifiable medical records, stripped of PII, can be sold to data brokers. When combined with as little as three or four data points from other databases, medical records can be conclusively linked to a specific individual. A well-known example of this occurred in 1997 when William Weld, a former governor of Cambridge, Massachusetts, supported the commercial release of 135,000 PII stripped state employee health records along with those of their families covered under the same state medical insurance program by the Massachusetts Group Insurance Commission (GIC) for the purpose of improving healthcare and controlling costs.[95] Then Massachusetts Institute of Technology student, now Harvard University privacy professor, Latanya Sweeney, cross referenced the GIC records with Cambridge, Massachusetts voter records and she was able to identify William Weld medical records. Adding a bit of theatrics to her discovery, Dr. Sweeney mailed Governor Weld's medical records to his office. Dr. Sweeney

later went on to show that about 87% of US citizens could be uniquely identified by three facts: zip code, date of birth, gender.[96] This process has become known as re-identification. Re-identification critics claim instances like Governor Welds are limited to high profile public figures but re-identification advocates have proven that high profile and low profile personal re-identification is only a function of data points. More data points make identification easier.

A recent *Issues in Information Systems* data brokerage exploratory literature review tallied the total world-wide data brokers at over 4,000 world-wide with an estimate of 2,500-4,000 firms in the US alone. The review further cited that:

> As of April 2017, there were an estimated 3.8 billion Internet users (Kemp, 2017). Each of these Internet users generates a vast amount and variety of digital data each day. According to Forbes, "More data has been created in the past two years than in the entire previous history of the human race" (Marr, 2016, para. 4). It has been estimated that 1.7 megabytes of new information will be created each second of the day for every human on the planet by the year 2020 (Marr, 2016).[97]
> In 2012, the data broker industry generated 150 billion dollars in revenue which was twice the size of the entire intelligence budget for the U.S. Government.[98]

Heretofore, much of the data broker industry focused business models on personal consumer data collection to reap the financial reward this type of information has to offer through targeting advertising and marketing value. The DOD still has use for this kind of information for precision targeting efforts required to find and fix individual high value targets (HVI), i.e., GPC foreign adversary individual Advanced Persistent Threat (APT) group members. There is cyber activity attribution value associated with tracking the whereabouts and activities of APT members. However, it is only a matter of time before data brokers recognize the market potential globally proliferated sensors and raw technical collection data capabilities they provide. Advances in mobile information technology (IT) hardware which increase telecommunication network data carrying capacity will enable a future technical intelligence data collection boom and the data brokers will capitalize the IT infrastructures newfound data capacity. Through

supporting a higher data transmission content and throughput rate, technologies like 5th generation (5G) telecommunications networks advance connectivity concepts like the Internet of Things (IoT), which "…foresees the interconnection of billions of things by extending the interaction between humans and applications to a new dimension of communication with things."[99] Hyper-connectivity, an IT industry term which includes the IoT, Web of Things, and Internet of Everything, will integrate multi-layer digital networks with all aspects of society and industry in the years to come.[100]

Data brokers leveraging these technologies and data collection concepts will also be a windfall to CICO supporting JIPOE in Joint Operations Phase 0. Entire areas of adversaries wired and wireless cyber networks might already be mapped by witting or unwitting foreign nationals who inadvertently collected the raw data through the course of their everyday lives by using of software applications whose publishers have existing data broker relationships. The data brokers need only identify this requirement to software publishers who then would re-write how the device applications use existing hardware sensors to collect technical data. Theoretically, this process could be completed in a device software update push.

Data brokers are able to execute cyberspace information collection operations in all three layers of cyberspace. In the physical layer the collection involves raw sensor data and unique device identifiers. From an antennae standpoint this is the radio frequencies and their received signal strength indicators (RSSI) decibel values at a given geographic location over time and space. From device standpoint this might be any information in the OSI physical, data link, or network layers such as a media access control (MAC) address identifier assigned to a network interface controller (NIC). In the logical layer, data brokers would record information such as IP address connectivity history, browser site history, cross site tracking via cookies and information

in other similar categories. The user layer is less relevant to technical data collection but would involve individual analysis of consumer habits and preferences in addition to travel and location history in much the same way the advertising industry conducts targeted advertising. Users in a specific geographic areas of interest might be influenced to adopt certain data broker affiliated applications.

These are simply the existing 'products' available on the open commercial market. There are scenarios in which a DOD contractor or the DOD itself could create a contract with specific requirements tailored to intelligence collection pertinent to specific aspects of each layer or interrelations and combinations of each. The ease and speed with which software developers could develop solutions for these requirements is enabled by SDR and SDN. The most important aspect of this idea is that it is all voluntary or indirect. The consumer consents at some level to the use of their device for collecting said data. The DOD is a customer and is not tasking the consumer to go certain places or complete specific functions. Rather, the consumer is offered a higher premium or a free service, e.g. Facebook, on a revolving and periodic basis based on their digital and geographic lifestyle characteristics. In this manner, DOD or its affiliates exert control based on the premium rate or level of service provided.

4.4 DATA ACQUISITION VIA PUBLIC PRIVATE PARTNERSHIP (PPP)

Farther along the JDCEF curve is technical cyber data collection via USG contractors specifically employed to collect information on adversaries' cyber infrastructure through CO. This way of CICO seems to be an existing strength within the proposed DOD JDCEF. USG-contractor analysis shows that contractors play critical roles in intelligence/reconnaissance and planning/mission support.[101] Different from DOD cyber information or SIGINT collection operations conducted by Joint Service personnel, DOD civilians, or even tasked HUMINT

sources, and cyber operations contractors are currently employed by the USG and exist somewhere between private military companies and private security companies. Cyber operations contractors have been an integral part of developing US cyber capabilities and will continue to be for the foreseeable future. Open source Omnibus contract solicitation records "… provide the most detailed insight publicly available to date about the contractual relationship between (the USG) and private cybersecurity contractors regarding offensive cyber operations in a military context."[102] In April 2015, CYBERCOM solicited proposals to award $475 million worth of contracts to outside private corporations to "…assist in the deliberate planning, coordination, and synchronization of Offensive Cyber Operations (OCO), Defensive Cyber Operations (DCO), and operation of the DODIN (Department of Defense Information Networks… Additionally, the contractor shall assist in providing maneuver, fires and effects through the application of capabilities in and through the cyber domain."[103] A few years later in 2017, estimates for the cyber threat intelligence market were as high as USD 1 billion.[104]

A presumption with USG contractors assisting CYBERCOM with CO is that the contractors are also actively conducting CICO and thereby collecting and sharing intelligence information regarding adversary networks. ManTech is a possible example of this. The USG awarded ManTech a USD $250 million contract in 2015 to assist in training cyber operations personnel.[105] In front of a picture of uniformed (presumably Air Force) personnel, ManTech's website advertises a cyber focus area as "Cyber: Tackling rising cyber threats with offense-informed defense. ManTech empowers networks and personnel with solutions and training that make cyber-attacks 'dead on arrival.'"[106] ManTech's website previously stated ManTech (provides) "…intelligence and operations, counterintelligence, information operations, and cyber-warfare."[107] Complimenting ManTech's CNO assistance with C-OPE, C-ISR, and CNE

type functions are companies like Endgame which identifies targetable computer systems in foreign countries. More precise descriptions of Endgame's role describe it as not conducting CNA but "…the intelligence it provides can give clients the information they need to carry out their own strikes."[108] This is exactly the type of function filled by CICO and CNE.

4.5 DATA ACQUISITION VIA CYBER OPERATIONS

The NSA, CIA, CYBERCOM, and the Joint Force maintain high functioning means of collecting cyber data via government owned and operated CO platforms. These platforms are policy makers' preferred weapon of choice when it comes to most OCO. The chief shortcoming of these means is that they are narrow in focus and often take months of high level bureaucratic approval prior to execution. PE, including the C-ISR and C-OPE necessary to execute CNE operations, often takes months or years to complete and requires more relative risk compared to the more passive broad scope approaches proposed above. This is true for both remote and local CNE operations. Entities executing local CNE operations in a physical domain are often limited in their geographic reach when operating in non-permissive or semi-permissive environments. Furthermore, there is a lack of coordinated effort among USG components to track the APT groups cybersecurity experts expect to fill a dominant role in GPC over the next decade. Private cybersecurity firms arguably maintain better public APT profiles than does the USG. A 2019 threat intelligence report from private cybersecurity firm FireEye even goes so far as to suggest that APT 41 is a Chinese state-backed espionage group which also tracks targeted individuals and conducts physical domain surveillance to obtain intelligence information which supports CO through CNE.[109] In this example, multi-domain intelligence collection operations are used to support CICO.

The Joint Force would be wise to more fully implement a combined intelligence approach to CO. In a May, 2019 meeting between the CTIIC directors, intelligence community members, and industry leaders on the topic of cyber deterrence, the Federal Bureau of Investigation (FBI) Cyber Division Deputy Assistant Director advocated a holistic intelligence attribution approach using (primarily) cyber domain derived intelligence data and only from data analysis versus a collection perspective.[110] Conducting effective JIPOE and supporting CICO will require a coordinated intelligence collection approach for the Joint Force to remain left of bang on CA and espionage timelines. Combined, inter-agency coordinated multi-source intelligence collection supporting C-ISR and C-OPE will provide invaluable indications and warnings related to an adversary's operational posture which may indicate likelihood hostile cyber activity. Intelligence professionals assert that timeliness and specificity of attack prediction and, by extrapolation, attribution are increasingly difficult in the modern OE.[111] This difficulty has some intelligence practitioners advocating beyond multi-disciplined intelligence analysis or mixed collection[112] for what is proposed as combined intelligence collection doctrine, an adaptation of combined arms in maneuver warfare.[113] This is aptly described as coordinated and mutually enabling multi source intelligence collection activities, i.e., each collection activity is designed to linearly enable subsequent activities and laterally enable associated activities. Collectively, combined intelligence collection information related to a single APT would be more effective than simply analyzing multi-source disaggregated threat information collected in an uncoordinated or haphazard manner. Consider the 2018 DOJ indictment against members of the Russian Federation Main Intelligence Directorate (GRU), case 18-263, US v. Aleksei Sergeyevich Morenets. The US federally charged Russian GRU officers with international hacking and executing associated influence and disinformation operations. The indictment

alleges that Russian GRU "close access" hacking teams traveled to various target foreign locations to compromise computer networks used by anti-doping and sporting officials in addition to networks of organizations investigating Russia's use of chemical weapons.[114] Language from the indictment reads,

> When the conspirators' remote hacking efforts failed to capture log-in credentials, or if the accounts that were successfully compromised did not have the necessary access privileges for the sought-after information, teams of GRU technical intelligence officers, including Morenets, Serebriakov, Sotnikov, and Minin, traveled to locations around the world where targets were physically located. Using specialized equipment, and with the remote support of conspirators in Russia, including Yermakov, these close access teams hacked computer networks used by victim organizations or their personnel through Wi-Fi connections, including hotel Wi-Fi networks. After a successful hacking operation, the close access team transferred such access to conspirators in Russia for exploitation.[115]

This Russian GRU operation is a superlative example of combined intelligence and CICO used to support information operations as part of a broader hybrid warfare strategy; Russian GRU operatives later manipulated and publicly released information obtained in the hacks to undermine legitimacy of the World Anti-Doping Agency (WADA). In this example, the Russian team represents an APT. DOD combined intelligence collection operations targeting the APT might have provided indications and warnings about the APT's operational posture. More importantly, the operations would have answered key questions: What can changes in that posture indicate about the likelihood of hostile activity? Secondarily, how can that information enable CICO which provide digital threat information on APT activities? Lastly, how can US decision makers use APT indications and warnings to conduct OCO, denying APT maneuver space in the cyber domain? In the Russian example, combined intelligence collection operations might have monitored the movement of the Russian GRU operatives and tracked their activities for indicators of target selection. Sensitized targets might have been alerted and prepared for any variety of DCO. A multi-disciplined intelligence entity such as a threat aligned Joint Interagency

Task Force (JIATF) dedicated to filling US cyber adversary posture intelligence gaps and executing subsequent CNE operations against APTs in Joint Force Phase 0 would effectively integrate combined intelligence collection and analysis principles with the maneuver warfare combined arms concept. For example, JIATF-41, named after APT-41, would be a tit for tat USG entity specifically charged with using JDCEF intelligence information to execute precision operations to deter, deny, or defeat APT-41 in a holistic manner, outside of cyberspace domain confines. Broad scope JDCEF data would be critical for a JIATF of this proposed size to maintain requisite agility and operational reach to counter or provide flexible response options against an APT.

5 CONCLUSION

There are various monikers of the now ubiquitous data broker aphorism, 'If you're not paying for a service or product, chances are that you're the product'. Contemporary data broker industry experts debate who originally coined the saying and the accuracy of its meaning but the message seems intuitive. Consumers generate data. Data is worth money. Private corporations have figured out a way to commoditize consumer data into commercially viable forms. Lastly, data commoditization has created a multi-billion dollar industry which is expected to grow for years to come. The Joint Force and intelligence community should heed this industry trend and harness it through a novel approach to conducting JIPOE in phase 0, particularly via the incorporation of Big Data, discussed through this paper as PAI/CAI.

The argument for the DOD's increased and systematic use of PAI/CAI begins with conclusions about the contemporary operational environment. Within today's environment, GPC hybrid warfare concepts bias US GPC adversaries towards exploiting asymmetric advantages inherent to CO executed in the gray zone. Evidence for this is apparent in the aforementioned

examples of Chinese and Russian doctrine. Empirical data also substantiate this assessment and seem to support CO as a low risk form of engagement which consistently prove to be non-escalatory in nature. It is evident that DOD CICO needs to systemically leverage broader sources of information and collection avenues given these conclusions and commercial industry experts' prognostications for how emerging technologies will expand access into the cyber domain. The JDCEF proposed in this paper illustrates a possible solution to what systematic gray zone CICO might look like.

The open market and data broker (PAI/CAI) echelons within the JDCEF model provide for both low risk and distributed collection approaches as a ways to execute broad scope CICO within contested areas of the cyber domain. More importantly, these CICO approaches are passive while involving private industry, consumer consent, and an implicit, non-escalatory nature. As a data collection framework, the JDCEF is founded upon sound economic principles. Use of JDCEF open market and data broker echelons to conduct CICO provides economy of scale and allows for the more efficient tasking of potential combined intelligence CNE enabling entities such as JIATF-41 to track and, or, combat a wide variety of APTs.

The JDCEF proposed in this paper provides a start to answering two of CYBERCOM's 2018 Cyber Symposium questions highlighted at the beginning of this paper. Ultimately, the principle hurdle to JDCEF implementation in its proposed form will need surmounted in a legal forum. DOD CO practitioners and the judge advocate lawyers advising them must view PAI/CAI as consensually released or published information. Vague and out of date consumer data privacy laws provide ways to leverage Big Data under current restrictions imposed by The Data Privacy Act of 1974 and The USA Freedom Act of 2015. DOD's use of PAI/CAI to conduct CICO in this regard would not be considered government overreach. Here, it is

important to consider a transactional ‘purchase’ as being unequivocally different from government ‘collection’. This concept is summarized in one statement, ‘I Agree.’, the colloquially phrased consent consumers give to software applications’ publishers for use of a software platform. That consent is the explicit permission users’ give for their device software to access their device sensors to collect information from the users on behalf of the software publisher. Consent is the ultimate reason why government owned and operated platforms directly conducting Phase 0 CICO should become a marginalized activity during future hybrid conflict. The private sector is already legally providing the information or the means to obtain it.

Endnotes

[1] US Cyber Command (CYBERCOM), "USCYBERCOM 2018 Cyberspace Strategy Symposium Proceedings," (Washington, DC: Headquarters US Cyber Command, 2018), 10.

[2] Lyle J. Morris, Michael J., Mazarr, Jeffrey W. Hornung, Stephanie Pezard, Anika Binnendijk, Marta Kepe, *Gaining Competitive Advantage in the Gray Zone: Response Options for Coercive Aggression Below the Threshold of Major War*. (Santa Monica, CA, USA: RAND National Defense Research Institute, 2019), iii, https://www.rand.org/pubs/research_reports/RR2942.html.

[3] Frank Hoffman, "Examining Complex Forms of Conflict: Gray Zone and Hybrid Challenges," Prism : A Journal of the Center for Complex Operations 7, no. 4 (November 1, 2018, 41. http://search.proquest.com/docview/2156325964/.

[4] P.W. Singer, Allan Friedman, *Cybersecurity and Cyberwar* (New York: Oxford University Press, 2014), 111.

[5] Gavin, Rusty. "Cybersecurity for Cloud-Based SCADA." *Control Engineering* 65, no. 8 (August 1, 2018), 51, http://search.proquest.com/docview/2131579200/.

[6] The Tallinn Manual or, 'Tallinn Manual on the International Law Applicable to Cyber Warfare' is a study of how international law applies to cyberspace. A team of approximately twenty international legal experts wrote the manual at the invitation of the Tallinn, Estonia-based NATO Cooperative Cyber Defence Centre of Excellence. Chicago University Press published the manual in April 2013.

[7] Michael N. Schmitt, Liis Vihul, The Nature of International Law Cyber Norms (December 1, 2014), Tallinn Papers No. 5 (NATO Cooperative Cyber Defence Centre of Excellence, Dec. 2014), 30, Available at SSRN: https://ssrn.com/abstract=2543520.

[8] Ibid., 30.

[9] Edwin Djabatey, "U.S. Offensive Cyber Operations against Economic Cyber Intrusions: An International Law Analysis – Part I," Just Security, last modified June 11, 2019, https://www.justsecurity.org/64875/u-s-offensive-cyber-operations-against-economic-cyber-intrusions-an-international-law-analysis-part-i/.

[10] Josh Fruhlinger, "The OPM hack explained: Bad security practices meet China's Captain America," last modified November 06, 2018, https://www.csoonline.com/article/3318238/the-opm-hack-explained-bad-security-practices-meet-chinas-captain-america.html.

[11] Brian Ulicny, "Today's enterprises face increasing risk of state-sponsored cyberattacks," Thomson Reuters Labs (blog), last modified January 14, 2019, https://blogs.thomsonreuters.com/answerson/state-sponsored-cyberattacks/.

[12] Christopher Whyte, Brandon Valeriano, Benjamin Jensen, Ryan Maness, "Rethinking the Data Wheel: Automating Open-Access, Public Data on Cyber Conflict," *2018 10th International Conference on Cyber Conflict*, NATO CCD COE Publications, Tallinn, 2018, 2.

[13] DOD cyber doctrine is so relatively new that terms, definitions, and acronyms are still changing. Within the past 10 years, CNO (CNA, CNE, CND) has transitioned to CO (OCO, DCO). Cyberspace Information Collection Operations and, or, Cyberspace Information Collection are not yet included in the DOD Dictionary of Military and Associated Terms or Joint Publication 3-12: Cyberspace Operations. Cyberspace Information Collection is formally addressed in the secondary source document, United States Army War College Center for Strategic Leadership, *Strategic Cyberspace Operations Guide*, (Washington, DC: Headquarters US Army, June 1, 2016), 18. The term is not formally abbreviated but will be abbreviated as CICO for the remainder of this paper.

[14] United States Army War College Center for Strategic Leadership, *Strategic Cyberspace Operations Guide*, (Washington, DC: Headquarters US Army, June 1, 2016), 18.

[15] Josh Fruhlinger, "The OPM hack explained: Bad security practices meet China's Captain America," last modified November 06, 2018, https://www.csoonline.com/article/3318238/the-opm-hack-explained-bad-security-practices-meet-chinas-captain-america.html.

[16] US Cyber Command (CYBERCOM), "Achieve and Maintain Cyberspace Superiority: Command Vision for US Cyber Command," (Washington, DC: Headquarters US Cyber Command, 2018), 4.

[17] Headquarters Department of Defense, *Summary: Department of Defense Cyber Strategy* (Washington, DC, 2018), 1.

[18] Headquarters Department of Defense, *Cyberspace Operations*, Joint Publication 3-12 (Washington, DC: Headquarters Department of Defense, June 08, 2018), I-3.

[19] Headquarters Department of Defense, *Special Operations*, Joint Publication 3-05 (Washington, DC: Headquarters Department of Defense, July 16, 2014), IV-4.

[20] Headquarters Department of the Army, *Intelligence Operations*, Field Manual 2-0 (Washington, DC: Headquarters Department of the Army, July 2018), 3-1.

[21] "The Global Operating Model comprises four layers: contact, blunt, surge, and homeland. These are, respectively, designed to help us compete more effectively below the level of armed conflict; delay, degrade, or deny adversary aggression; surge war-winning forces and manage conflict escalation; and defend the U.S. homeland." (Headquarters Department of Defense, *Summary of the 2018 National Defense Strategy of The United States of America: Sharpening the American Military's Competitive Edge*. (Washington, DC: Department of Defense, 2018), 7.)

[22] Frank G. Hoffman, C*onflict in the 21st Century: The Rise of Hybrid Wars*, (Arlington, VA, USA: Potomac Institute for Policy Studies, 2007), 8, https://www.potomacinstitute.org/images/stories/publications/potomac_hybridwar_0108.pdf

[23] Headquarters Department of Defense, *Irregular Warfare: Countering Irregular Threats*, Joint Operations Concept v 2.0 (Washington, DC: Headquarters Department of Defense, May 17, 2010), 9.

[24] Headquarters Department of Defense, *Doctrine for the Armed Forces of the United States*, JP 1 (Washington, DC: Headquarters Department of Defense, July 12, 2017), I-5.

[25] Max Roser, "Percentage of years in which the 'Great Powers' fought one another, 1500-2015," Our World In Data, last modified May 18, 2019, https://ourworldindata.org/uploads/2013/08/ourworldindata_percentage-of-years-in-which-the-great-powers-fought-one-another-1500–2000.png.

[26] Steven Pinker, *The Better Angels of Our Nature: Why Violence Has Declined* (New York, New York: Penguin Books, 2012), 1.

[27] Jack S. Levy, William R. Thompson, *The Arc of War: Origins, Escalation, and Transformation*. (Chicago: University of Chicago Press, 2011), 2.

[28] Jim Garamone, "Military Must Be Ready to Confront Hybrid Threats, Intel Official Says," US Department of Defense, last modified September 4, 2019, https://www.defense.gov/Explore/News/Article/Article/1952023/military-must-be-ready-to-confront-hybrid-threats-intelligence-official-says/.

[29] CrowdStrike, *2019 Global Threat Report: Adversary Tradecraft and the Importance of Speed*, (Sunnyvale, CA: CrowdStrike, 2019), 32.

[30] Director of National Intelligence, *Worldwide Threat Assessment of the Intelligence Community*, (Washington DC: Office of the Director of National Intelligence (ODNI), February 13, 2018), 5.

[31] Kenneth Katzman, *Iran Sanctions*, CRS Report for Congress, Committee on Foreign Affairs, House of Representatives, One Hundred Twelfth Congress, First Session, on H.R. 1905 and H.R. 2105 (Washington, DC: Congressional Research Service, October 15, 2012), Summary page, https://apps.dtic.mil/dtic/tr/fulltext/u2/a584872.pdf.

[32] Headquarters Department of Defense, *Joint Operations*, Joint Publication 3-0 (Washington, DC: Headquarters Department of Defense, October 22, 2018), V-8.

[33] Ibid., V-9.

[34] Headquarters Department of Defense, *Cyberspace Operations*, Joint Publication 3-12 (Washington, DC: Headquarters Department of Defense, June 08, 2018), II-6.

[35] Ibid., II-11.

[36] Headquarters Department of Defense, *Joint Intelligence*, Joint Publication 2-0 (Washington, DC: Headquarters Department of Defense, October 22, 2013), I-5.

[37] Director of National Intelligence, *National Intelligence Strategy of the United States of America*, (Washington DC: Office of the Director of National Intelligence (ODNI), 2019), 5.

[38] Ibid., 11.

[39] Milton Mueller, Andreas Schmidt, Brenden Kuebris, "Internet Security and Networked Governance in International Relations," *International Studies Review* 15 (2013), 100.

[40] Federal Trade Commission, *Complaint, Request for Investigation, Injunction, and Other Relief, Submitted by: The Electronic Privacy Information Center*, (Washington, DC: Federal Trade Commission, 2015), 5.

[41] Ash Turner, "How many smartphones are in the world?," last modified February 25, 2020, https://www.bankmycell.com/blog/how-many-phones-are-in-the-world#sources.

[42] Benjamin Carton, Joannes Mongardini, Yinqun Li, *A New Smartphone for Every Fifth Person on Earth: Quantifying the New Tech Cycle*, IMF Working Paper, The International Monetary Fund Research Department WP/18/22, 2018, 2.

[43] CPU World, "AMD Athlon 64 X2 3800+ (Socket 939, rev. E4) specifications," last modified November 16, 2019, http://www.cpu-world.com/CPUs/K8/AMD-Athlon%2064%20X2%203800+%20-%20ADA3800DAA5BV%20(ADA3800BVBOX).html.

[44] Apple.com, "iPhoneXR," last modified February 26, 2020, https://www.apple.com/iphone-xr/specs/.

[45] Ibid., 1.

[46] Markus Dillinger, Kambiz Madani, Nancy Alonistioti, *Software Defined Radio Architectures, Systems and Functions*, (Hoboken: Wiley and Sons, 2003), xxxiii.

[47] Donald J. Trump, National Security Strategy (NSS) (Washington, DC: White House, 2017), 28, https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf.

[48] Charles Dunlap Jr., "Lawfare 101: A Primer," *Military Review* (May-June 2017), 9.

[49] Ibid., 11.

[50] Jamie Pinchot, Adnan Chawdhry, Karen Paullet, "Data Privacy Issues in the Age of Data Brokerage: An Exploratory Literature Review," *Issues in Information Systems*, 19 no. 3 (2018), 97.

[51] Jill Goldenziel, Manal Cheema, "The New Fighting Words?: How U.S. Law Hampers the Fight Against Information Warfare," *Journal of Constitutional Law*, 22 no. 1 (November 2019), 116.

[52] Jacqueline Klosek, *Data Privacy in the Information Age* (Westport: Quorum Books, 2000), 130.

[53] Ibid., 130.

[54] Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change* (Washington, DC: Federal Trade Commission, March 2012), 67.

[55] Federal Trade Commission, *Data Brokers: A Call for Transparency and Accountability* (Washington, DC: Federal Trade Commission, 2014), 7.

[56] Jamie Pinchot, Adnan Chawdhry, Karen Paullet, "Data Privacy Issues in the Age of Data Brokerage: An Exploratory Literature Review," *Issues in Information Systems*, 19 no. 3 (2018), 97.

[57] Woodrow Hartzog, *Privacy's Blueprint: The Battle to Control the Design of New Technologies* (Cambridge: Harvard University Press, 2018), *63*.

[58] Office of the Director of National Intelligence, *Civil Liberties and Privacy Guidance for Intelligence Community Professionals: Properly Obtaining and Using Publicly Available Information,"* (Washington, DC: Office of the Director of National Intelligence, July 2011), 12.

[59] Steven Melendez, Alex Pasternack, "Here are the data brokers quietly buying and selling your personal information," last modified March 02, 2019, https://www.fastcompany.com/90310803/here-are-the-data-brokers-quietly-buying-and-selling-your-personal-information.

[60] Drew Fitzgerald, Sarah Krouse, "FCC Probe Finds Mobile Carriers Didn't Safeguard Customer Location Data," Wall Street Journal, last modified February 27, 2020, https://www.wsj.com/articles/fcc-probe-finds-mobile-carriers-didnt-safeguard-customer-location-data-11582830682?mod=searchresults&page=1&pos=2.

[61] Headquarters Department of Homeland Security, *Privacy Impact Assessment Update for the Border Surveillance Systems (BSS)*, DHS/CBP/PIA-022(a), (Washington, DC, 2018), https://www.dhs.gov/sites/default/files/publications/privacy-pia-cbp022-bss-september2018.pdf

[62] Jill Goldenziel, Manal Cheema, "The New Fighting Words?: How U.S. Law Hampers the Fight Against Information Warfare," *Journal of Constitutional Law*, 22 no. 1 (November 2019), 116.

[63] Jacqueline Klosek, *Data Privacy in the Information Age* (Westport: Quorum Books, 2000), 130.

[64] Christl Wolfie, "Corporate Surveillance in Everyday Life: How Companies Collect, Combine, Analyze, Trade, and User Personal Data on Billions," (Vienna: Cracked Labs, June 2017), https://crackedlabs.org/en/corporate-surveillance.

[65] Fred Kaplan, *Dark Territory: The Secret History of Cyber War*, read by Malcolm Hillgartner, 2016, audiobook, Disc 5 | also at https://time.com/darkterritory/)

[66] Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008, 50 U.S.C. § 1881a Sec 702d (1).

[67] American Civil Liberties Union et. al. v. James R. Clapper et. al., 14-42 US Court of Appeals 2nd Circuit 168-1, 72 (2015). | accessed at https://pdfserver.amlaw.com/nlj/NSA_ca2_20150507.pdf

[68] Drew Fitzgerald, "T-Mobile Vows to Fight FCC Fines for Location Sharing," Wall Street Journal, last modified February 28, 2020, https://www.wsj.com/articles/t-mobile-vows-to-fight-fcc-fines-for-location-sharing-11582921450?mod=hp_lista_pos1.

[69] Ibid., 1.

[70] Jacqueline Klosek, *Data Privacy in the Information Age* (Westport: Quorum Books, 2000), 130.

[71] Woodrow Hartzog, *Privacy's Blueprint: The Battle to Control the Design of New Technologies* (Cambridge: Harvard University Press, 2018), *63*.

[72] Dara Massicot, "Anticipating a New Russian Military Doctrine in 2020: What it Might Contain and Why it Matters," War on the Rocks, last modified September 9, 2019, https://warontherocks.com/2019/09/anticipating-a-new-russian-military-doctrine-in-2020-what-it-might-contain-and-why-it-matters/.

[73] Akhilesh Ganti, "Efficient Frontier," Investopedia, last modified April 1, 2019, https://www.investopedia.com/terms/e/efficientfrontier.asp.

[74] Tim Maurer, *Cyber Mercenaries: The State, Hackers, and Power* (Cambridge: Cambridge University Press, 2018), 25.

[75] Marshall Hargrave, "Crowdsourcing," Investopedia, last modified July 08, 2019, https://www.investopedia.com/terms/c/crowdsourcing.asp

[76] Seti@home, "About SETI@home," University of California, last modified 2020, https://setiathome.berkeley.edu/sah_about.php.

[77] Bitcoinmining.com, "How Bitcoin Mining Works," last modified 2018, https://www.bitcoinmining.com/.

[78] MarketsandMarkets, "Cryptocurrency Market by Offering (Hardware: GPU, FPGA, ASIC, & Wallet, and Software), Process (Mining and Transaction), Type, Application (Trading, Remittance, Payment: Peer-to-Peer Payment, Ecommerce, and Retail), and Geography - Global Forecast to 2024," Marketsand Markets Research Private Ltd., 2020, https://www.marketsandmarkets.com/Market-Reports/cryptocurrency-market-158061641.html.

[79] Cristin Dorgelo, Brian Forde, "By the People, for the People: Crowdsourcing to Improve Government," White House Office of Science and Technology Policy, partnered content on WIRED, last modified February 01, 2020, https://www.wired.com/insights/2014/04/people-people-crowdsourcing-improve-government/#start-of-content.

[80] Melanie Hicken, "What information is the government buying about you?," CNN Money, last modified October 30, 2013, https://money.cnn.com/2013/10/30/pf/government-data-broker/index.html.

[81] Office of the Director of National Intelligence, *A White Paper on the Key Challenges in Cyber Threat Intelligence: Explaining the "See it, Sense it, Share it, Use it" approach to thinking about Cyber Intelligence,* (Washington, DC: Office of the Director of National Intelligence, September 14, 2018), 1, https://www.dni.gov/files/CTIIC/documents/White_paper_on_Cyber_Threat_Intelligence_ODNI_banner_10_30_2018.pdf.

[82] Office of the Director of National Intelligence, *"ODNI Home: Features – CTIIC Quick Facts,"* (Washington, DC: Office of the Director of National Intelligence, last modified February 27, 2020, https://www.dni.gov/index.php/ctiic-features.

[83] Justin Wolfers, Eric Zitzewitz, "Prediction Markets," *Journal of Economic Perspectives* 18, no. 2 (Spring 2004), 107.

[84] Ibid, 108.

[85] Halton, Clay, "Wisdom of Crowds," Investopedia, last modified July 23, 2019, https://www.investopedia.com/terms/w/wisdom-crowds.asp.

[86] Maurice Dawson, Mohamed Eltayeb, Marwan Omar, *Security Solutions for Hyperconnectivity and the Internet of Things*. (Hershey, PA: IGI Global, 2017), 95.

[87] Valeria Insinna, "Inside America's Dysfunctional Trillion-Dollar Fighter-Jet Program, New York Times, last modified August 21, 2019, https://www.nytimes.com/2019/08/21/magazine/f35-joint-strike-fighter-program.html.

[88] Andrew McGonigles, Thomas Wilkes, Tom Pering, Jon Willmott, Joseph Cook, Forrest Mims, Alfio Parisi, "Smartphone Spectrometers," *Sensors* 18 no. 223 (2018), www.mdpi.com/journal/sensors.

[89] Milosz Krasinski, "The Long Tail Effect theory in practice explained," Milosz Krasinski (blog), last modified February 28, 2020, https://miloszkrasinski.com/the-long-tail-effect-theory-in-practise-explained/.

[90] Nicholas Mumm, "Crowdsourcing: A New Perspective on Human Intelligence Collection in a Counterinsurgency," Small Wars Journal – Small Wars Foundation, last modified 2018, https://smallwarsjournal.com/node/12036.

[91] Jamie Pinchot, Adnan Chawdhry, Karen Paullet, "Data Privacy Issues in the Age of Data Brokerage: An Exploratory Literature Review," *Issues in Information Systems*, 19 no. 3 (2018), 92.

[92] *What Information Do Data Brokers Have on Consumers, and How Do They Use it?: Hearing of The Senate Committee on Commerce, Science, and Transportation,* (2013) (testimony of Pam Dixon, Executive Director, World Privacy Forum), https://www.worldprivacyforum.org/2013/12/testimony-what-information-do-data-brokers-have-on-consumers/.

[93] Ibid, 5.

[94] Jamie Pinchot, Adnan Chawdhry, Karen Paullet, "Data Privacy Issues in the Age of Data Brokerage: An Exploratory Literature Review," *Issues in Information Systems*, 19 no. 3 (2018), 92.

[95] Madhumita Murgia, "How data brokers sell your identity," TEDx Exeter, NPR, podcast video, 2020 https://www.ted.com/talks/madhumita_murgia_how_data_brokers_sell_your_identity?language=en.

[96] Daniel Barth-Jones, "The "Re-identification" of Governor William Weld's Medical Information: A Critical Re-examination of Health Data Identification Risks and Privacy Protections, Then and Now," rev. (pre-publication draft – working paper, SSRN, 2015), 5, available online at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2076397.

[97] Jamie Pinchot, Adnan Chawdhry, Karen Paullet, "Data Privacy Issues in the Age of Data Brokerage: An Exploratory Literature Review," *Issues in Information Systems*, 19 no. 3 (2018), 92.

[98] Jamie Pinchot, Adnan Chawdhry, Karen Paullet, "Data Privacy Issues in the Age of Data Brokerage: An Exploratory Literature Review," *Issues in Information Systems*, 19 no. 3 (2018), 95.

[99] Maurice Dawson, Mohamed Eltayeb, Marwan Omar, *Security Solutions for Hyperconnectivity and the Internet of Things*. (Hershey, PA: IGI Global, 2017), 13.

[100] Ibid., 2.

[101] Tim Maurer, *Cyber Mercenaries: The State, Hackers, and Power* (Cambridge: Cambridge University Press, 2018), 76.

[102] Ibid., 76.

[103] Ibid., 71.

[104] Ibid., 71.

[105] Ibid., 74.

[106] Mantech, "Focus Area: Cyber," Mantech Corporate Website, last modified February 28, 2020, https://www.mantech.com/.

[107] Tim Maurer, *Cyber Mercenaries: The State, Hackers, and Power* (Cambridge: Cambridge University Press, 2018), 74.

[108] Ibid., 76.

[109] FireEye, *Double Dragon: APT41, a dual espionage and cybercrime operation*, Special Report (Milpitas: FireEye, 2019), 3.

[110] Aspen Institute, "Cyberattack Deterrence," in *Cyberattack Deterrence* (Washington, DC, USA: The Aspen Institute, May 29, 2019), 5:30, https://www.c-span.org/video/?461166-1/cyberattack-deterrence&start=1983.

[111] James J. Wirtz, *Understanding Intelligence Failure: Warning, response, and deterrence*. (New York: Routledge, 2017), 113.

[112] Headquarters Department of Defense, *Joint and National Intelligence Support to Military Operations*, JP 2-01 (Washington, DC: Headquarters Department of Defense, July 05, 2017), III-29.

[113] James J. Wirtz, *Understanding Intelligence Failure: Warning, response, and deterrence*. (New York: Routledge, 2017), 113.

[114] Headquarters Department of Justice, "Justice News: U.S. Charges Russian GRU Officers with International Hacking and Related Influence and Disinformation Operations," DOJ Office of Public Affairs, last modified October 4, 2018, https://www.justice.gov/opa/pr/us-charges-russian-gru-officers-international-hacking-and-related-influence-and.

[115] Ibid., 1.

Glossary

Advanced Persistent Threat (APT). A broad term describing a computer network threat actor that gains unauthorized access to a computer network; APTs often targets the same adversary(s) in multiple attacks over time and space and remain undetected for an extended periods; APTs may be nation state, state-sponsored, or non-state sponsored groups.

Commercially Available Information (CAI). There is no common definition for CAI across the IC. Per the US Attorney General guidelines for the FBI regarding PAI, CAI is inferred to be any information available to the public by subscription or purchase. (ODNI Civil Liberties and Privacy Guidance for Intelligence Community Professionals: Properly Obtaining and using Publicly Available Information, July 2011) (Approved for public release by DNI Pre-Pub 20140708)

cyberspace exploitation. Actions taken in cyberspace to gain intelligence, maneuver, collect information, or perform other enabling actions required to prepare for future military operations. (JP 3-12, June 2018)

Computer Network Attack (CNA). Actions taken through the use of computer networks to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves. (JP 1-02, March 2012) CNE has since been removed from JP 1-02, February 2016 and JP 3-13, November, 2014. DOD Doctrine now encompasses CNA in OCO.

Computer Network Defense (CND). Actions taken to protect, monitor, analyze, detect, and respond to unauthorized activity within the Department of Defense information systems and computer networks. (JP 1-02, March 2012) CNE has since been removed from JP 1-02, February 2016 and JP 3-13, November, 2014. DOD Doctrine now encompasses CND in DCO.

Computer Network Exploitation (CNE). Actions taken through the use of computer networks to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves. (JP 1-02, March 2012) CNE has since been removed from JP 1-02, February 2016 and JP 3-13, November, 2014. DOD Doctrine now refers to CNE as cyberspace exploitation.

Cyber Information Collection. Actions that facilitate cyberspace operations primarily through deliberate network reconnaissance and surveillance or other enabling activities in and through cyberspace; activities in cyberspace conducted to gather intelligence from target and adversary systems; enabling activities conducted to plan and prepare for follow-on operations. (US Army War College Strategic Cyberspace Operations Guide, June 2016)

Cyber Information Collection Operations (CICO). Planned, coordinated, and sequenced activities conducted in support of Cyber Information Collection.

Cyber Intelligence Surveillance Reconnaissance (C-ISR). Cyber intelligence actions conducted to gather intelligence, integrate and synchronize the planning and implementation of: sensors and assets, processing systems, exploitation systems, and dissemination systems. (US Army War College Strategic Cyberspace Operations Guide, June 2016)

Cyber Operations (CO). All DOD operations conducted in and, or, through cyberspace regardless of their intended or actual effect.

Cyber Preparation of the Environment (C-OPE). Cyber activities conducted to gain and maintain access to systems and processes; to identify data and software, system configurations, network configurations; to position capabilities for follow-on actions. (US Army War College Strategic Cyberspace Operations Guide, June 2016)

Offensive Cyber Operations (OCO). Missions intended to project power in and through cyberspace. (JP 3-12, June 2018)

Defensive Cyber Operations (DCO). Missions to preserve the ability to utilize blue cyberspace capabilities and protect data, networks, cyberspace-enabled devices, and other designated systems by defeating on-going or imminent malicious cyberspace activity. Also called DCO. (JP 3-12, June 2018)

Irregular Warfare (IW). A violent struggle among state and non-state actors for legitimacy and influence over the relevant population(s). (JP 1, March 2013)

Hybrid Warfare. There is no hybrid warfare definition in Joint Doctrine. For this paper, hybrid warfare is generally multi-domain, kinetic, non-kinetic, conventional and irregular threats coordinated across a conflict continuum spanning war through peace.

Gray Zone. There is no gray zone definition in Joint Doctrine. For this paper the gray zone is a conceptual space where adversaries compete or fight with each other under the precepts of plausible deniability, ambiguous legal standards, or irregular, non-normalized methods.

Joint Data Collection Efficient Frontier (JDCEF). The JDCEF is a novel term proposed in this paper as an Intelligence Collection method modeled after the 1952 Nobel Laureate Harry Markowitz's Efficient Frontier economic model that relates asset risk to investment return.

Joint Intelligence Preparation of the Environment (JIPOE). The analytical process used by joint intelligence organizations to produce intelligence estimates and other intelligence products in support of the joint force commander's decision-making process. ((JP 1-02, February 2016; JP 3-05)

Preparation of the Environment (PE). An umbrella term for operations and activities conducted by selectively trained special operations forces to develop an environment for potential future special operations. Also called PE. (JP 3-05)

Publicly Available Information (PAI). There is no common definition for PAI across the IC. The US Attorney General guidelines for the FBI defines PAI as information that has been published or broadcast for public consumption, is accessible on-line or otherwise to the public, is available to the public by subscription or purchase, could be seen or heard by any casual observer, is made available at a meeting open to the public, or is obtained by visiting any place or attending any event that is open to the public. (ODNI Civil Liberties and Privacy Guidance for Intelligence Community Professionals: Properly Obtaining and using Publicly Available Information, July 2011) (Approved for public release by DNI Pre-Pub 20140708)

Bibliography

Apple.com, "iPhoneXR," last modified February 26, 2020, https://www.apple.com/iphone-xr/specs/.

Aspen Institute. "Cyberattack Deterrence." in *Cyberattack Deterrence*. Washington, DC, USA: The Aspen Institute, May 29, 2019. https://www.c-span.org/video/?461166-1/cyberattack-deterrence&start=1983.

Barth-Jones, Daniel. "The "Re-identification" of Governor William Weld's Medical Information: A Critical Re-examination of Health Data Identification Risks and Privacy Protections, Then and Now." rev. pre-publication draft – working paper, SSRN, 2015. Available online at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2076397.

Bitcoinmining.com. "How Bitcoin Mining Works." Accessed February 27, 2020, https://www.bitcoinmining.com/.

Carton, Benjamin, Joannes Mongardini, Yinqun Li. *A New Smartphone for Every Fifth Person on Earth: Quantifying the New Tech Cycle*. IMF Working Paper, The International Monetary Fund Research Department WP/18/22, 2018.

Clarke, Michael. "China's Application of the 'Three Warfares' in the South China Sea and Xinjiang." *Orbis* 63, no. 2 (January 01 2019): 187-208. https://doi.org/10.1016/j.orbis.2019.02.007.

Clarke, Richard A. *Cyber War: The Next Threat to National Security and What to Do About It*. New York, NY: First Ecco, HarperCollins Publishers, 2012.

CPU World. "AMD Athlon 64 X2 3800+ (Socket 939, rev. E4) specifications." accessed February 12, 2020. http://www.cpu-world.com/CPUs/K8/AMD-Athlon%2064%20X2%203800+%20-%20ADA3800DAA5BV%20(ADA3800BVBOX).html.

CrowdStrike. *2019 Global Threat Report: Adversary Tradecraft and the Importance of Speed*. Sunnyvale, CA: CrowdStrike, 2019.

Curran, Dylan. "Are your phone camera and microphone spying on you?" accessed February 23, 2020. https://www.theguardian.com/commentisfree/2018/apr/06/phone-camera-microphone-spying.

Dawson, Maurice, Mohamed Eltayeb, Marwan Omar. *Security Solutions for Hyperconnectivity and the Internet of Things*. Hershey, PA: IGI Global, 2017.

Dillinger, Markus, Kambiz Madani, Nancy Alonistioti. *Software Defined Radio Architectures, Systems and Functions*. Hoboken: Wiley and Sons, 2003.

Director of National Intelligence, *National Intelligence Strategy of the United States of America*, Washington DC: Office of the Director of National Intelligence (ODNI), 2019.

Director of National Intelligence, *Worldwide Threat Assessment of the Intelligence Community*, Washington DC: Office of the Director of National Intelligence (ODNI), February 13, 2018.

Djabatey, Edwin, "U.S. Offensive Cyber Operations against Economic Cyber Intrusions: An International Law Analysis – Part I," Just Security, accessed February 20, 2019, https://www.justsecurity.org/64875/u-s-offensive-cyber-operations-against-economic-cyber-intrusions-an-international-law-analysis-part-i/.

Dorgelo, Cristin, Brian Forde. "By the People, for the People: Crowdsourcing to Improve Government." White House Office of Science and Technology Policy, partnered content on WIRED, last modified February 01, 2020, https://www.wired.com/insights/2014/04/people-people-crowdsourcing-improve-government/#start-of-content.

Dunlap, Charles Jr., "Lawfare 101: A Primer," *Military Review* (May-June 2017).

Federal Trade Commission. *Complaint, Request for Investigation, Injunction, and Other Relief, Submitted by: The Electronic Privacy Information Center*. Washington, DC: Federal Trade Commission, 2015.

FireEye. *Double Dragon: APT41, a dual espionage and cybercrime operation*. Special Report. Milpitas: FireEye, 2019.

Fruhlinger, Josh. "The OPM hack explained: Bad security practices meet China's Captain America," accessed February 05, 2020, https://www.csoonline.com/article/3318238/the-opm-hack-explained-bad-security-practices-meet-chinas-captain-america.html.

Fitzgerald, Drew. "T-Mobile Vows to Fight FCC Fines for Location Sharing." Wall Street Journal, last modified February 28, 2020, https://www.wsj.com/articles/t-mobile-vows-to-fight-fcc-fines-for-location-sharing-11582921450?mod=hp_lista_pos1.

Fitzgerald, Drew, Sarah Krouse. "FCC Probe Finds Mobile Carriers Didn't Safeguard Customer Location Data." Wall Street Journal, accessed February 28, 2020, https://www.wsj.com/articles/fcc-probe-finds-mobile-carriers-didnt-safeguard-customer-location-data-11582830682?mod=searchresults&page=1&pos=2.

Ganti, Akhilesh. "Efficient Frontier." Investopedia, last modified April 1, 2019, https://www.investopedia.com/terms/e/efficientfrontier.asp).

Garamone, Jim. "Military Must Be Ready to Confront Hybrid Threats, Intel Official Says," US Department of Defense, accessed February 19, 2019,

https://www.defense.gov/Explore/News/Article/Article/1952023/military-must-be-ready-to-confront-hybrid-threats-intelligence-official-says/.

Gavin, Rusty. "Cybersecurity for Cloud-Based SCADA." *Control Engineering* 65, no. 8 (August 1, 2018): 50–52. http://search.proquest.com/docview/2131579200/.

Headquarters Department of Defense. *Cyberspace Operations*. JP 3-12. Washington, DC: Headquarters Department of Defense, June 08, 2018.

Headquarters Department of the Army. *Intelligence Operations*, Field Manual 2-0. Washington, DC: Headquarters Department of the Army, July 2018.

Headquarters Department of Defense. *Irregular Warfare: Countering Irregular Threats*. Joint Operating Concept v 1.0 (Washington, DC: Headquarters Department of Defense, September 11, 2007.

Headquarters Department of Defense. *Irregular Warfare: Countering Irregular Threat*. Joint Operating Concept v 2.0. Washington, DC: Headquarters Department of Defense, May 17, 2010.

Headquarters Department of Defense, *Joint Intelligence*. Joint Publication 2-0 Washington, DC: Headquarters Department of Defense, October 22, 2013.

Headquarters Department of Defense. *Joint Operations*. Joint Publication 3-0. Washington, DC: Headquarters Department of Defense, October 22, 2018.

Headquarters Department of Defense, *NDS Irregular Warfare Annex*, Joint Staff J-7 staff briefing, 2019, 2, https://www.jcs.mil/Portals/36/Documents/Doctrine/MECC2019/mecc2019day1brief8_iw.pdf?ver=2019-10-17-143158-750.

Headquarters Department of Defense. *Special Operations*, Joint Publication 3-05. Washington, DC: Headquarters Department of Defense, July 16, 2014.

Headquarters Department of Defense. *Summary of the 2018 National Defense Strategy of The United States of America: Sharpening the American Military's Competitive Edge.* Washington, DC: Department of Defense, 2019.

Headquarters Department of Defense. *Summary: Department of Defense Cyber Strategy.* Washington, DC, 2018.

Headquarters Department of Homeland Security. *Privacy Impact Assessment Update for the Border Surveillance Systems (BSS)*, DHS/CBP/PIA-022(a). Washington, DC, 2018. https://www.dhs.gov/sites/default/files/publications/privacy-pia-cbp022-bss-september2018.pdf.

Headquarters Department of Justice. "Justice News: U.S. Charges Russian GRU Officers with International Hacking and Related Influence and Disinformation Operations." DOJ Office of Public Affairs, last modified October 4, 2018, https://www.justice.gov/opa/pr/us-charges-russian-gru-officers-international-hacking-and-related-influence-and.

Hicken, Melanie. "What information is the government buying about you?" CNN Money. last modified October 30, 2013, https://money.cnn.com/2013/10/30/pf/government-data-broker/index.html.

Hoffman, Frank G. C*onflict in the 21st Century: The Rise of Hybrid Wars*. Arlington, VA, USA: Potomac Institute for Policy Studies, 2007, https://www.potomacinstitute.org/images/stories/publications/potomac_hybridwar_0108.pdf.

Hoffman, Frank. "Examining Complex Forms of Conflict: Gray Zone and Hybrid Challenges." *Prism : a Journal of the Center for Complex Operations* 7, no. 4 (November 1, 2018): 30–47. http://search.proquest.com/docview/2156325964/.

Hoffman, Frank. "On Not-So-New Warfare: Political Warfare vs Hybrid Threats," accessed January 29, 2020, https://warontherocks.com/2014/07/on-not-so-new-warfare-political-warfare-vs-hybrid-threats/.

Insinna, Valeria. "Inside America's Dysfunctional Trillion-Dollar Fighter-Jet Program." New York Times, accessed February 28, 2020, https://www.nytimes.com/2019/08/21/magazine/f35-joint-strike-fighter-program.html.

Kapusta, Philip. "The Gray Zone." *Special Warfare* 28 (October-December 2015), 18-25, https://www.soc.mil/SWCS/SWmag/archive/SW2804/October%202015%20Special%20Warfare.pdf.

Katzman, Kenneth. *Iran Sanctions.* CRS Report for Congress, Committee on Foreign Affairs, House of Representatives, One Hundred Twelfth Congress, First Session, on H.R. 1905 and H.R. 2105. Washington, DC: Congressional Research Service, October 15, 2012. https://apps.dtic.mil/dtic/tr/fulltext/u2/a584872.pdf.

Kofman, Michael. "Russian Hybrid Warfare and other Dark Arts," last accessed February 29, 2016, https://warontherocks.com/2016/03/russian-hybrid-warfare-and-other-dark-arts/.

Krasinski, Milosz. "The Long Tail Effect theory in practice explained." Milosz Krasinski (blog), last modified February 28, 2020, https://miloszkrasinski.com/the-long-tail-effect-theory-in-practise-explained/.

Levy, Jack S.; Thompson. *The Arc of War : Origins, Escalation, and Transformation*. Chicago: University of Chicago Press, 2011.

Lyle J. Morris, Michael J., Mazarr, Jeffrey W. Hornung, Stephanie Pezard, Anika Binnendijk, Marta Kepe, *Gaining Competitive Advantage in the Gray Zone: Response Options for Coercive Aggression Below the Threshold of Major War*. (Santa Monica, CA, USA: RAND National Defense Research Institute, 2019), iii, https://www.rand.org/pubs/research_reports/RR2942.html.

Mantech, "Focus Area: Cyber," Mantech Corporate Website, accessed February 28, 2020, https://www.mantech.com/.

MarketsandMarkets. "Cryptocurrency Market by Offering (Hardware: GPU, FPGA, ASIC, & Wallet, and Software), Process (Mining and Transaction), Type, Application (Trading, Remittance, Payment: Peer-to-Peer Payment, Ecommerce, and Retail), and Geography - Global Forecast to 2024." Marketsand Markets Research Private Ltd., 2020, https://www.marketsandmarkets.com/Market-Reports/cryptocurrency-market-158061641.html.

Massicot, Dara. "Anticipating a New Russian Military Doctrine in 2020: What it Might Contain and Why it Matters." War on the Rocks, accessed September 9, 2019, https://warontherocks.com/2019/09/anticipating-a-new-russian-military-doctrine-in-2020-what-it-might-contain-and-why-it-matters/.

Maurer, Tim. *Cyber Mercenaries: The State, Hackers, and Power*. Cambridge, UK: Cambridge University Press, 2018.

McGonigles, Andrew, et. al. "Smartphone Spectrometers." *Sensors* 18 no. 223 (2018), www.mdpi.com/journal/sensors.

Mueller, Milton, Andreas Schmidt, Brenden Kuebris. "Internet Security and Networked Governance in International Relations." *International Studies Review* 15, 2013.

Mumm, Nicholas. "Crowdsourcing: A New Perspective on Human Intelligence Collection in a Counterinsurgency." Small Wars Journal – Small Wars Foundation, last modified 2018, https://smallwarsjournal.com/node/12036.

Office of the Director of National Intelligence. *A White Paper on the Key Challenges in Cyber Threat Intelligence: Explaining the "See it, Sense it, Share it, Use it" approach to thinking about Cyber Intelligence.* Washington, DC: Office of the Director of National Intelligence, September 14, 2018. https://www.dni.gov/files/CTIIC/documents/White_paper_on_Cyber_Threat_Intelligence_ODNI_banner_10_30_2018.pdf.

Office of the Director of National Intelligence, *Civil Liberties and Privacy Guidance for Intelligence Community Professionals: Properly Obtaining and Using Publicly Available Information,* (Washington, DC: Office of the Director of National Intelligence, July 2011. (Originally marked UNCLASSIFIED//FOUO; approved for public release by DNI Pre-Pub 20140708)

Office of the Director of National Intelligence. *"ODNI Home: Features – CTIIC Quick Facts."* Washington, DC: Office of the Director of National Intelligence, accessed February 27, 2020. https://www.dni.gov/index.php/ctiic-features.

Paddock, Alfred H, and Army War College Carlisle Barracks PA. *Psychological and Unconventional Warfare, 1941-1952: Origins of a Special Warfare Capability for the United States Army,* November 1979. http://www.dtic.mil/docs/citations/ADA086801.

Pinchot, Jamie, et al. "Data Privacy Issues in the Age of Data Brokerage: An Exploratory Literature Review." *Issues in Information Systems* 19, no. 3 (2018), 92-100. http://www.iacis.org/iis/2018/3_iis_2018_92-100.pdf.

Pinker, Steven. *The Better Angels of Our Nature : Why Violence Has Declined* New York, New York: Penguin Books, 2012.

Roser, Max. "Percentage of years in which the 'Great Powers' fought one another, 1500-2015." Our World In Data, accessed February 01 2020, https://ourworldindata.org/uploads/2013/08/ourworldindata_percentage-of-years-in-which-the-great-powers-fought-one-another-1500–2000.png.

Schmitt, Michael N. and Vihul, Liis, The Nature of International Law Cyber Norms (December 1, 2014). Tallinn Papers No. 5 NATO Cooperative Cyber Defence Centre of Excellence, Dec. 2014. https://ssrn.com/abstract=2543520.

Schmitt, Michael N. *Tallinn Manual on the International Law Applicable to Cyber Warfare.*, 2013.

Schmitt, Michael N. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge: Cambridge University Press, 2017.

Seti@home, "About SETI@home," University of California, last modified 2020, (https://setiathome.berkeley.edu/sah_about.php).

Singer, P.W., Allan Friedman. *Cybersecurity and Cyberwar*. New York: Oxford University Press, 2014.

Trump, Donald J. *National Security Strategy (NSS).* Washington, DC: White House, 2017. https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf.

Turner, Ash. “How many smartphones are in the world?” last accessed February 25, 2020. https://www.bankmycell.com/blog/how-many-phones-are-in-the-world#sources.

Ulicny, Brian. “Today’s enterprises face increasing risk of state-sponsored cyberattacks,” Thomson Reuters Labs (blog), accessed February 20, 2019, https://blogs.thomsonreuters.com/answerson/state-sponsored-cyberattacks/.

United States Army War College Center for Strategic Leadership. *Strategic Cyberspace Operations Guide*. Washington, DC: Headquarters US Army, June 1, 2016.

US Cyber Command (CYBERCOM). “Achieve and Maintain Cyberspace Superiority: Command Vision for US Cyber Command.” Washington, DC: Headquarters US Cyber Command, 2018.

US Cyber Command (CYBERCOM). “USCYBERCOM 2018 Cyberspace Strategy Symposium Proceedings.” Washington, DC: Headquarters US Cyber Command, 2018.

Whyte, Christopher, Brandon Valeriano, Benjamin Jensen, Ryan Maness. “Rethinking the Data Wheel: Automating Open-Access, Public Data on Cyber Conflict.” *2018 10th International Conference on Cyber Conflict*. NATO CCD COE Publications, Tallinn, 2018.

Wolfers, Justin, Eric Zitzewitz. “Prediction Markets.” *Journal of Economic Perspectives* 18 no. 2 (2004), 107-126.

Wolfie, Christl. “Corporate Surveillance in Everyday Life: How Companies Collect, Combine, Analyze, Trade, and User Personal Data on Billions.” Vienna: Cracked Labs, June 2017. https://crackedlabs.org/en/corporate-surveillance.