palgrave pivot

The U.S. Cybersecurity and Intelligence Analysis Challenges

John Michael Weaver

palgrave macmillan

The U.S. Cybersecurity and Intelligence Analysis Challenges

John Michael Weaver

The U.S. Cybersecurity and Intelligence Analysis Challenges

palgrave
macmillan

John Michael Weaver
Department of History and Political Science
York College of Pennsylvania
York, PA, USA

ISBN 978-3-030-95840-4 ISBN 978-3-030-95841-1 (eBook)
https://doi.org/10.1007/978-3-030-95841-1

This Palgrave Macmillan imprint is published by the registered company Springer Nature Switzerland AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

Preface

The forthcoming analysis in this book looked at taking a conventional understanding of the four instruments of national power (diplomacy, information, military, and economic measures/D.I.M.E.) and turning the tables to see how potential adversarial powers could use these against the national security interests of the United States. Moreover, it focused on qualitative research regarding the cyber threat that has continually beleaguered this nation by malevolent actors mostly over the last seven years. The study also affords consideration to how potential adversarial non-state actors and nation-states can implement the instruments of national power through the application of a new model named the York Intelligence Red Team Model-Cyber (Modified) [YIRTM-C (M)] using sources guided by the Federal Qualitative Secondary Data Case Study Triangulation Model to arrive at results.

John Michael Weaver
Department of History
and Political Science
York College of Pennsylvania
York, PA, USA

Contents

About the Author

John Michael Weaver is an Associate Professor of Intelligence Analysis at York College of Pennsylvania (USA), a retired DOD civilian from the United States' Intelligence Community and has served as an officer in the U.S. Army (retiring at the rank of lieutenant colonel). He has lived and worked on four continents and in 19 countries spending nearly eight years overseas (on behalf of the US government). His experience includes multiple combat deployments, peace enforcement, peacekeeping, humanitarian relief, and disaster assistance support in both conventional and unconventional/non-traditional units. John has trained and certified multinational NATO reconnaissance teams based in The Netherlands, Germany, and Spain for worldwide deployment in full-spectrum mission sets. He has also personally led several reconnaissance missions throughout Europe, the Middle East, and Asia (including multiple missions in Afghanistan). He has received formal training/certification in the following areas from the US Department of Defense: Survival/Evasion/Resistance/Escape (high risk), communications equipment & communications planning (FM radio, landline & satellite communications, encryption, and the use of cryptographic devices), digital camera use & digital photography courses, US Joint Forces Command joint intelligence course, US Special Operations Command counterintelligence awareness course (USSOCOM CI), US Joint Forces Command counterintelligence awareness training (USJFCOM CI), counterinsurgency course, joint antiterrorism course, defense against suicide

bombing course, dynamics of international terrorism, homeland security and defense course, the joint special operations task force course (JSOTF), defensive driving course, vehicle emergency drills (battle drills), composite risk management, the airborne and air assault schools, and more. Additionally, he graduated from NATO's Combined Joint Operations Center course in Oberammergau Germany, the Air Command and Staff College, and the Joint & Combined Warfighting School. John earned a Bachelor of Arts degree in business management from Towson University in 1990, graduated from Central Michigan University with a Master of Science in Administration degree in 1995, earned a Master of Operational Arts and Science degree from the U.S. Air Force's Air University in 2004, and graduated from the University of Baltimore with a Doctorate in Public Administration in 2013.

List of Figures

CHAPTER 1

Introduction and Background

Abstract The use of the cyber domain for conflict is a relatively recent phenomenon. This chapter introduces the reader to cybersecurity threats and provides background information.

Keyword CNA · CNE · CNO · Cyber

This work looks to implement what Boyer calls the scholarship of integration (Glassick 2000). It does so by considering a series of micro-case studies looking at four nation-states and two non-state actors. One of the prevailing issues of contemporary times centers on the issue of cyber threats confronting western nations (Weaver 2017). When focusing attention to the topic of information and cyber-warfare, information is often seen as far more advantageous than money and is even more valued than currency because it is through information that one can attain more wealth (Bruce et al. 2004, 11). It can influence opinions, shape actions, and through using what is now termed "deep fakes" can modify the actual presentation of speeches by leaders to convey anything other than what they actually stated (with extreme realism).

These threats are increasingly more disruptive and destructive, and most nations' infrastructure is extremely vulnerable to them (GAO-16-332 2016). As individuals, companies, and governments at all levels rely

J. M. Weaver, *The U.S. Cybersecurity and Intelligence Analysis*,
https://doi.org/10.1007/978-3-030-95841-1_1

more on information technology, collaborative tools like Google Drive (Google Docs, Google Sheets, and the view/edit function), and Kubernetes, information could become vulnerable to exploitation, and as a result, a lot of inherent risks exists in today's world. Compounded with the use of asymmetric and hybrid warfare, these threats are real.

The Cyber Domain

The use of the cyber domain for conflict is a relatively recent phenomenon. Indeed, debates are ongoing as to whether cyber should be regarded as a fifth-domain analogous to the physical military theaters of air, land, sea, and space and whether there has yet been any real incident akin to conflict on those domains meeting the threshold of what constitutes warfare (McGuffin and Mitchell 2014). The burgeoning of cyber is marked by several incidents and prolific cyber-weapons: the Central Intelligence Agency's (CIA's) use of the 'logic bomb' is often considered the first case of cyber operations concerning national security; these also include the North Atlantic Treaty Organization's (NATO's) PROMIS; the emergence of non-state hackers; the Russian's 'Moonlight Blaze' (which gained information about American missile targeting systems); and the Chinese 'Titan Rain,' just to name but a few (Lakomy 2013, 108). A critical event concerning the militarization of cyber within classic geopolitics is Russia's actions in Estonia, which is regarded by some as the first 'cyber war' "since computer networks were used to paralyze the critical infrastructure of a nation-state" (Lakomy 2013, 106). Lastly, the famous 'Stuxnet' virus is routinely referenced as the beginning of a "new era of cyber-warfare and suggested that this new type of cyber-weapon had a similar meaning for international security as the bombing of Hiroshima and Nagasaki" (Lakomy 2013, 106). This statement underscored that cyber, like nuclear weapons over time, has changed the actual structural conditions of conflict and warfare while it increased the 'grey zone' range of operations once reserved for classical espionage. An empirical question regarding cyber is to what degree will cyber continue to be used, and within what capacities, in terms of offensive attacks (Weaver and Johnson 2020). While most concerns for cyber defense examine the integration of civilian infrastructure with the internet of things (IoT), offensive cyber tactics, techniques, and procedures (TTPs) may be used to attack a military's increasing dependence on networked technology, even that which is offline. Cyber may also play a part in hybrid warfare, where attackers may

"leverage this expanded attack surface through target sets that generate effects in both the information and physical domains" through direct or *nth* level multiplier effects (Gendron 2013; Leuprecht et al. 2019, 389). These actors could also help enhance their anonymity using virtual private network (VPN) technology, The Onion Router (TOR) browser (and surfing the 'dark web'), etc., making it very difficult to trace the origin of cyber events.

Thus, cyber operations can be utilized to undermine the integrity of a country by hindering the state's ability to pursue its interests (however defined) through immobilization, which may also see the manifestation of physical destruction in the classic sense of warfare (Weaver and Johnson 2020). Further, cyber operations could help undermine the stability of a society that is reminiscent of classic disinformation campaigns. This might be true as the diversification of actors and their access to technology, combined with decreases of violent geopolitical conflict between major state powers (Kshetri 2013), suggests that digital and cyber-based threats will increase in sophistication and prevalence as they are used to elicit specific political, social, and economic outcomes (Weaver and Johnson 2020).

Politically, Lakomy essentially argues that "Cyber-warfare challenges the security policies of all industrial states and the lack of a clear international mechanism to coordinate responses has increased the need for independent action to be undertaken in a spinoff of an arms race. In short, each state is forced to develop its plan of action with or without its allies" (2013, 108). Thus, cyber dangers may prioritize national action and self-interest from a classical focus on *raison d'état* as the international order is too slow to adapt and other competitive pressures may emerge (e.g., trade wars) (Weaver and Johnson 2020).

The seeming lack of coordinated policy between allied states on cybersecurity may partially be linked to this structural shift in addition to the seeming inability of international mechanisms, including organizations, regimes, and laws, to adapt to what is seen as the new structural reality (Weaver and Johnson 2020). This inability for the liberal international order to adapt to rising challenges, and by extension, the difficulties encountered by individual states, is partially due to the rapid acceleration of technological change. As Adams argues, "owing to market incentives, innovation in functionality is outpacing innovation in security" (2016, 1). However, the lack of coordinated international policy on cybersecurity may also be the result of the discursive dominance of cyber-'war' rather

than, say, cyber-'crime' (Levin and Goodrick 2013). The former often is indicative of competition among nation-states, firmly entrenching cybersecurity in the realm of national defense whereas the latter suggests the need to combat illegitimate criminal organizations and enterprises that may hold relevance to national security but also is inclusive of the cooperation of non-military actors, such as policing forces across various boundaries, both state and non-state. Overall, the amalgam of this structural shift inherent to the wide array of cyber technologies, and the rhetorical focus on warfare and military theaters has led many nations to pursue a cybersecurity strategy predicated on 'resilience' underpinned by public–private partnerships (P2Ps) to induce industry to innovate and take up part of the defense burden given that a great deal of cyber is privately owned (e.g., CADSI 2019), creating a "polycentric governance architecture" (Dupont 2018, 26).

However, Carr (2016) argues that there is an inherent challenge in this strategy, mostly due to contradictions between the goals (of private capital) and the needs (of national security), or more broadly, the difference between private interests and public goods (Weaver and Johnson 2020). Carr goes on to argue that a central problem to P2Ps is "the expectation that the private sector will invest in cybersecurity beyond its cost/benefit analysis to fully accommodate the public interest - in other words, to ensure national security" (2016, 60). Likewise, Grayson and O'Higgins (2018, 30) make the point that governments need to play a central role in cybersecurity efforts through the incorporation of private actors rather than relying on them. However, even when governments are accorded a central role in defending their populations against cyber threats, this may create a 'wicked problem' for liberal democracies such as that of the United States. The 'wicked problem' refers to the contradiction between enabling freedom and ensuring security in democratic societies, or "where to draw the line between adequate security, reasonable cost, and personal freedom" (Malone and Malone 2013, 158). The 'wicked problem' is especially problematic when considering the ideational aspect of cyber threats, i.e., operations designed to create disinformation among society, and which may be combined with other forms of attack (more recently termed 'hybrid warfare'). Cyber threats believed to be linked to disinformation campaigns are especially problematic due to the fact that they undermine and challenge the ontological security of societies (the taken-for-granted faith that the world is as it appears, which underlies our sense of trust in that world and its representative