Cyber Counterintelligence in the Contemporary Security Threatscape

A proposal submitted for the degree of Doctor of Philosophy

Courteney J. O'Connor

October 2015

Cyber Counterintelligence in the Contemporary Security Threatscape

The role of counterintelligence in modern security concerns is to identify, undermine and counter foreign and/or hostile actors' intelligence efforts so as to reduce the level of threat represented by those actors. Traditionally, counterintelligence has been undertaken by State actors in response to the actions of other States or State-representative parties. The profusion of non-State actors in the late nineteenth and early twentieth centuries has seen the focus of counterintelligence efforts expand beyond the traditional State-centric model. Non-State actors are now capable of affecting the security of the State through intense intelligence collection in cyberspace, and are also increasingly the subject of intelligence collection and exploitation themselves. The rise of cyberspace as an exploitable domain not exclusive to the State, in concert with the dynamic profusion and diffusion of information technologies has resulted in an operational domain wherein policy and understanding has failed to keep pace with functional capability. Given these parameters, has cyber counterintelligence policy and practice developed apace to cyber exploitation capabilities? How are actors, at different levels of analysis, understanding and employing cyber counterintelligence measures? This thesis will examine the history, development and diffusion of cyber counterintelligence practices and technologies and how this field relates to and influences contemporary notions of individual, national, and international security.[1]

Research foci

In order to contextualize the field and practice of cyber counterintelligence, this research will begin with an examination of the cyber domain. Once this domain, also called cyberspace, has been delineated this thesis will continue by defining and examining the concept and analyze the placement of cyber counterintelligence in the wider counterintelligence and security disciplines. The research will include an examination of the history and development of cyber counterintelligence starting with the securitization of the cyber domain by the United States of America in the 1970s (Dunn Cavelty, 2013, p. 364). It will examine the profusion and diffusion of cyber counterintelligence practices and technologies at the individual, organized group, corporate, and State levels and assess the impact of these upon the concept of security.

Once an understanding of cyber counterintelligence has been reached and contextualized by assessing the utility and employment of cyber counterintelligence practices and processes by four different actors, this thesis will consider the contemporary security threatscape in relation to the cyber domain. The use or nonuse

[1] For contemporary perspectives on security, see Collins (2010) and Dannreuther (2013).

of cyber counterintelligence affects individual, corporate, national and international security in a variety of ways and to varying degrees of significance. Cyberspace is increasingly being used as an attack vector by State and non-State actors and thus far has been primarily contextualized in terms of criminal activity, terrorist activity, and a method of covert mass surveillance. Given the military, political, and societal importance of cyber security it is crucial that further studies examine the role and methods of cyber counterintelligence before it is precipitated by necessity. Through the investigation proposed by this thesis, it will be possible to extrapolate from contemporary security concerns how cyber counterintelligence will affect the future of security and offer a foundation for further research.

Key Literature

Cyberspace and Cyber Security

The existing body of literature surrounding cyberspace and its pertinence to national and international security is extensive and growing. Among those already surveyed, four works stand out as comprehensive and relevant treatments of the subject matter. *Cyberpower and National Security*, edited by Franklin Kramer et al. and published in 2009 provides a thorough examination of cyberspace and its evolution into an element of national power (Kramer, Starr, & Wentz, 2009). The manner in which cyberpower is wielded by the State, and the issues and vulnerabilities that same power represents are also thoroughly treated. While information security is considered in several of the essays in this key text and presumably deemed of crucial importance in the contemporary era, cyber intelligence and counterintelligence as separate fields are not considered in significant depth.

Nazli Choucri provides an excellent examination of the integration of cyberspace and cyber security concerns into contemporary international relations in her 2012 publication *Cyberpolitics in International Relations.* Both theoretically and empirically grounded, Choucri's text deals extensively with how cyberspace and its associated risks have affected and likely will continue to affect international relations in terms of cooperation and conflict. While the text does not examine intelligence or counterintelligence in cyberspace it is an extensive and thorough assessment of the current state of cyber politics *per se* (Choucri, 2012).

Myriam Dunn Cavelty, in her contribution to *Contemporary Security Studies*, examines the contemporary situation of and attitudes toward cyber security or insecurity (Dunn Cavelty, 2013). Beyond defining types of threat such as viruses and worms, Dunn Cavelty identifies three interrelated cyber-security discourses. The first is the technical discourse, relating to the malicious software and systems intrusions that have computers and computer networks as primary referent objects. The second discourse relates to crime and espionage undertaken *via* cyberspace, whose primary referent objects Dunn Cavelty identifies as business networks and classified

information/government networks. The third and final discourse is that of military/civil defence, relating to the primary referent objects of critical informational infrastructures and military networks. Dunn Cavelty gives a chronological overview of major instances of cyber crime, espionage, and conflict and after a brief overview of information security practices concludes that the risks posed by cyberspace have been overstated.

The fourth text, co-authored by Peter W. Singer and Allan Friedman and entitled *Cybersecurity and Cyberwar: What Everyone Needs to Know* is written more for popular understanding than the other texts mentioned here but is no less informative or academically rigorous for it. The text is separated into three broad categories; what cyberspace is, how it works, and what security risks and threats exist; why cyber security matters in the broad scheme of international security and the lessons that can be learned from past incidences; what could be done to reduce the relative insecurity of cyberspace and to whom the responsibility for security belongs (Singer & Friedman, 2014).[2]

Counterintelligence

Mark M. Lowenthal's treatment of counterintelligence in his quintessential text *Intelligence: From Secrets to Policy* provides on overview of the counterintelligence discipline and process (Lowenthal, 2012). While Lowenthal's text is rooted in his experience with and knowledge of the United States intelligence community, his conclusions are generalizable to the counterintelligence process worldwide. He outlines the advantages and disadvantages of counterintelligence practices, and the dangers of a counterintelligence process that is lacking. Lowenthal offers a detailed view of traditional counterintelligence but does not examine the contemporary concern over cyber security and modern cyber counterintelligence practice or processes.

Counterintelligence and National Strategy by Michelle K. Van Cleave, while focused on the American counterintelligence process and history, is a well-researched and rigorous view of counterintelligence as a tool of national strategy. As well as outlining the functions of modern counterintelligence, Van Cleave examines the U.S. national security strategy under the Bush administration and links those security concerns with strategic counterintelligence practice (Van Cleave, 2007). After overviewing the fragmented history of American counterintelligence, she goes on to outline a more efficient counterintelligence structure and offer prescriptions for future counterintelligence policy.

[2] For further information on information technologies and warfare, see Singer (2010). For a perspective on cyber crimes, see Goodman (2015).

John Ehrman authored a paper in a 2009 concerning the lack of a theoretical foundation to counterintelligence studies, entitled *What are we talking about when we talk about counterintelligence?* Rather than claim to have created a theory of counterintelligence, Ehrman discusses the necessary elements such a theory would need to cover. Ehrman thoroughly examines the definition and elements of counterintelligence, though Ehrman's belief that counterintelligence is an analytic discipline in the first instance rather than an operational discipline colours the discussion (Ehrman, 2009).

Cyber counterintelligence

Petrus Duvenage, Sebastian von Solms and Manuel Corregedor presented a paper entitled *The Cyber Counterintelligence Process: A Conceptual Overview and Theoretical Proposition* at the 14th European Conference on Cyber Warfare and Security in July 2015. The paper proposes a clear outline of what the cyber counterintelligence process should look like, and notes that while States have been practicing cyber counterintelligence for approximately two decades, as an academic field the literature is lacking (Duvenage, von Solms, & Corregedor, 2015). Duvenage and von Solms have previously presented, at the 2014 Conference, a paper conceptualizing cyber counterintelligence as an integral element of multi-disciplinary counterintelligence which lays an excellent foundation for further research (Duvenage & von Solms, 2014).

Johan Sigholm and Martin Bang offer a more technical understanding of cyber counterintelligence in their 2013 article *Towards Offensive Cyber Counterintelligence: Adopting a Target-Centric View on Advanced Persistent Threats*. Sigholm and Bang argue that in order to be effective, particularly in the context of military intelligence, the cyber counterintelligence process needs to be fast and offensive. The paper puts forward a framework for offensive cyber counterintelligence that could also be applied to the intelligence communities beyond the military (Sigholm & Bang, 2013).[3]

Methodology

This research will examine the history and development of cyber counterintelligence practices and technologies from a securitization perspective. Initially, this thesis will focus on how cyberspace was securitized for individuals, organized groups, corporations, and States. The acceptance of cyberspace as a vulnerable domain and the development of the cyber security industry have affected how contemporary actors understand cyber counterintelligence. This thesis will provide an examination

[3] For further material on the importance of cyber counterintelligence, see Duvenage & von Solms (2013); Boawn (2014); Rudner (2013).

of the history of cyber counterintelligence practice, stemming from the initial securitization of cyberspace in the 1970s by the American military to the modern day. The methodology for this research will primarily involve discourse analysis investigating and analyzing what literature exists in order to identify trends and provide appropriate context to the issue.

The securitization of cyberspace influenced the development and diffusion of practices, processes and technologies normally associated with State intelligence apparatuses.[4] Cyber counterintelligence is now employed at the individual, corporate, national and international levels of analysis using interrelated processes and technologies. How actors utilize (or fail to utilize) cyber counterintelligence at each of these levels of analysis affects both the concept of and actual individual, national and international security. The main resources for this research will be the nascent body of literature surrounding the field of cyber counterintelligence, and the existing bodies of literature surrounding cyberspace and cyber security and traditional counterintelligence.

Despite the importance of both the academic study and professional practice of cyber counterintelligence, the subject as a field of research can only be classified as emergent, and requiring extensive and intensive investigation and analysis. The relative lack of literature pertaining specifically to cyber counterintelligence can be mitigated by extensive research into the fields of traditional counterintelligence practice and methods, as well as those of cyberpower and cyber security that have been more extensively researched than cyber counterintelligence. The extant academic literature in these and associated fields is extensive and will provide a solid foundation for research. Grey literature, (understood as published or unpublished conference papers, research theses, newspaper and journal articles) as well as government and non-governmental organization publications will be examined for corporate, national and international approaches to and concerns over cyber counterintelligence. National security strategies and national cyber security strategies will be analyzed, and existing domestic, bilateral and/or multilateral agreements concerning cyberspace will also be examined. The published reports and data of trusted cybersecurity firms such as Kaspersky Lab and Symantec will also be utilized (Kaspersky Lab, 2015) (Symantec, 2015). In addition and particularly useful for the study of cyber counterintelligence are online news sources such as Foreign Policy and Wired Magazine, notable for their overarching views on contemporary security and the quality of their contributors (Wired.com, 2015) (Foreign Policy, 2015).

Merits and Objectives

[4] For an examination of the laws of warfare as pertain to cyberspace, see Dinniss (2014). Fur further material on cyber warfare see Rid (2013); Andress & Winterfeld (2011).

It is evident from the relative dearth of existing academic literature in the field of cyber counterintelligence that further research in the area is crucial to better our understanding of the concerns of contemporary international security. While associated disciplines such as traditional counterintelligence, general cyber security and the growing importance of cyberspace and cyber power have been more extensively investigated and researched; cyber counterintelligence has suffered a comparative lack of attention in scholarly circles.

While the security of cyberspace is widely acknowledged as being of the utmost importance to the security of industrialized and industrializing nations in the twenty-first century, comparatively little is understood about the domain in comparison the more traditional domains of land, sea, air and space. Within the traditional security field, counterintelligence is regarded as a necessary exercise and element of the pursuit of national security and has been analyzed extensively. Conversely, despite the ubiquitous nature of cyberspace for the individual, the organized group, the corporation and the State, cyber counterintelligence has, to date, not received a similar degree of attention. Current scholarship in the field is nascent, and tends to focus on the technical or the theoretical; this investigation seeks to understand the role of cyber counterintelligence in contemporary reality and security. By examining how cyber counterintelligence is understood and employed by different actors, and how the utilization will affect individual, national and international concepts of security this research will add to the existing body of literature and provide a foundation for further research.

In order to adequately understand contemporary security it is crucial that further research into the field of cyber counterintelligence be undertaken, and the results of that research integrated into the overarching field of intelligence as it pertains to security. This research will add to the existing body of knowledge surrounding cyber counterintelligence, particularly pertaining to how different actors utilize cyber counterintelligence and how that use affects concepts and security in real terms. The ability to attribute attacks, undermine foreign exploitation attempts and avoid future cyber exploitation is already, and will continue to be an important element of security. Cyber security will only become more important in the future, and this investigation will add to both academic and professional understandings of the importance of counterintelligence in cyberspace.

Bibliography

Andress, J., & Winterfeld, S. (2011). *Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners.* Waltham: Syngress.

Boawn, D. L. (2014). *Cyber Counterintelligence, Defending the United States' Information Technology and Communications Critical Infrastructure from Chinese Threats.* 2014: ProQuest LLC.

Choucri, N. (2012). *Cyberpolitics in International Relations.* Cambridge: The MIT Press.

Collins, A. (Ed.). (2010). *Contemporary Security Studies* (3rd Edition ed.). Oxford: Oxford University Press.

Dannreuther, R. (2013). *International Security: The Contemporary Agenda* (2nd Revised Edition ed.). Cambridge: Polity Press.

Dunn Cavelty, M. (2013). Cyber-security. In A. Collins (Ed.), *Contemporary Security Studies* (3rd Edition ed., pp. 362-378). Oxford: Oxford University Press.

Duvenage, P., & von Solms, S. (2014). Putting Counterintelligence in Cyber Counterintelligence: Back to the Future. In A. Liaropoulos, & G. Tzihrintzis (Eds.), *Proceedings of the 13th European Conference on Cyber Warfare & Security* (pp. 70-79). Reading: Academic Conferences and Publishing International Limited.

Duvenage, P., & von Solms, S. (2013). The Case for Cyber Counterintelligence. *International Conference on Adaptive Science and Tehnology* , 1-8.

Duvenage, P., von Solms, S., & Corregedor, M. (2015). The Cyber Counterintelligence Process: A Conceptual Overview and Theoretical Proposition. In N. Abouzakhar (Ed.), *Proceedings of the 14th European Conference on Cyber Warfare & Security* (pp. 42-51). Reading: Academic Conferences and Publishing International Limited.

Ehrman, J. (2009). What are We Talking About When We Talk about Counterintelligence? *Studies in Intelligence , 53* (2), 5-20.

Foreign Policy. (2015). *Foreign Policy*. Retrieved from Foreign Policy: http://foreignpolicy.com/

Goodman, M. (2015). *Future Crimes.* London: Bantam Press.

Harrison Dinniss, H. (2014). *Cyber Warfare and the Laws of War.* New York: Cambridge University Press .

Kaspersky Lab. (2015). *Internet Security Center*. Retrieved from Kaspersky Lab: http://www.kaspersky.com/internet-security-center

Kramer, F. D., Starr, S. H., & Wentz, L. K. (Eds.). (2009). *Cyberpower and National Security.* Dulles: Potomac Books, Inc.

Lowenthal, M. M. (2012). *Intelligence: From Secrets to Policy* (5th Edition ed.). Thousand Oaks: CQ Press.

Rid, T. (2013). *Cyber War Will Not Take Place.* London: C. Hurst & Co. (Publishers) Ltd.

Rudner, M. (2013). Cyber-Threats to Critical National Infrastructure: An Intelligence Challenge. *International Journal of Intelligence and Counterintelligence , 26* (3), 453-481.

Sigholm, J., & Bang, M. (2013). Towards Offensive Cyber Counterintelligence: Adopting a Target-Centric View on Advanced Persistent Threats. *European Intelligence and Security Informatics Conference (EISIC)* , 166-171.

Singer, P. W. (2010). *Wired For War: The Robotics Revolution and Conflict in the 21st Century.* London: Penguin Books Ltd.

Singer, P. W., & Friedman, A. (2014). *Cybersecurity and Cyberwar: What Everyone Needs to Know.* New York: Oxford University Press.

Symantec. (2015). *Security Response*. Retrieved from Symantec: https://www.symantec.com/security_response/

Van Cleave, M. K. (2007). *Counterintelligence and National Strategy.* Washington D.C.: National Defense University Press.

Wired.com. (2015). *Security*. Retrieved from Wired: http://www.wired.com/category/security