Bring on the Cyber Attacks – The increased predatory power of the restrained red queen in a nation-state cyber conflict

Dr. Rosemary A. Burk
Dr. Jan Kallberg

ABSTRACT

The militarized and contested Internet with a multitude of state-sponsored cyberattacks can generate an evolutionary process when the targeted nation is strengthened by the abundance of information it receives from the attacks. When the targeted nation restrains from retaliating against the attacking adversarial state its systems are perfected, meanwhile the attacking state is denied the feedback needed to stay current and pose a long-term threat. The targeted nation has increased its potential to go from prey to predator, when the accrued knowledge far exceeds the attacker, and the game has changed. The targeted nation can then strike back far superior on the initial attacker compared to the initial attacker's first moves. In contrast to the Red Queen hypothesis, our Restrained Red Queen model illustrates the adaptive advantage of a targeted nation that decides to selectively counter-strike its aggressor. The reticent targeted nation has benefited from restraining to counter-strike and increases its own survivability by embracing the initial attacks as information that can be converted to superiority over time.

Keywords–cyber evolution; cyber defense; information assurance; cyberwar theory; cyber conflict; cybersecurity

I. INTRODUCTION

This article challenges the common perception that cyberattacks are per default bad and dangerous, and instead argues that cyberattacks carry information vital for the refinement and evolution of the targeted state. Since the dawn of the common Internet, the fear of cyberattacks has been the focal point for the cybersecurity discourse. Cyberattacks carry the seeds for technological development and evolution that drive the ability to go from prey to predator in future cyberwar.

Dr. Rosemary Burk is a Senior Biologist with the U.S. Fish and Wildlife Service, Ecological Services Division in Pacific Northwest Region. Sheearned a Ph.D. in Biology from the University of North Texas with a specialization in aquatic ecology and environmental science. She has co-authored several articles that have linked failed cyber defense and environmental consequences including *Failed Cyberdefense: The Environmental Consequences of Hostile Acts*, which was published by U.S. Army *Military Review* in 2014.

of cyber resilience. The Internet is an ever-evolving online environment with a multitude of actors, but attacks on core nation state functionalities and systems that can degrade the state require substantial resources and intent, which radically limit the number of potential actors to nation states and state-sponsored proxies. The heavy cost and level of dedicated resources to destabilize or shut down a critical system by another state is not in reach for unfunded hackers, terrorists, and cyber criminals.[1] These nation state destabilizing attacks are limited to heavily funded and able actors, which translates to nation states and their agencies.

Cyberattacks that seek to undermine government stability, remove military advantages such as satellite communication, degrade the global information grid and geospatial awareness, impact the financial system, and provide a leverage at a critical juncture in either a low intensity or escalated nation state conflict limits the number of actors. The severity of these attempts and attacks exclude nation states with lower geopolitical postures, and non-state actors. The traditional cyber criminals and the bulk of Internet attacks tend to be vandalism or pursuit of monetary gain, and are in this conflict a background noise of limited importance.

The militarized and contested Internet with a multitude of state-sponsored cyberattacks can generate an evolutionary process when the targeted nation is strengthened by the abundance of information it receives from the attacks. This information is converted through security standards and knowledge consolidation to a higher level of defensive abilities, and the attacks have then strengthened the targeted states. If a nation state instead was denied the cyberattacks that provide information stimulus in adaptive behavior, it will become weakened and over time accumulate numerous unaddressed system vulnerabilities.

Dr. Jan Kallberg is Assistant Professor of American Politics in the Department of Social Sciences and Cyber Policy Fellow at the Army Cyber Institute at West Point. He holds a Ph.D. in Public Affairs and a Master's of Political Science from the University of Texas at Dallas; and a JD/LL.M. from Stockholm University. Prior to joining the West Point faculty, Jan was a researcher and Post-Doc at the Cyber Security Research and Education Institute, Erik Jonsson School of Engineering and Computer Science, at the University of Texas at Dallas under Dr. Bhavani Thuraisingham.

Dr. Kallberg's research interest is the intersection between public leadership and cyber capabilities; especially offensive cyber operations as an alternative policy option. His personal website is www.cyberdefense.com.

Cyberattacks in their varied forms, appeal to sensationalism due to the tenets of the malicious online activity. [2] Targeted states are perceived not only as risking to lose their citizens' privacy, but also industrial and financial strength, and geopolitical advantages. Furthermore, as every society becomes more reliant upon networked equipment, the reach of cyberattacks has passed a point of being not only a personal threat, but increasingly a national security threat. [3]

Until now, the vast majority of cyberattacks have been of low complexity, lacking precise targeting, and mainly degrade and have non-critical services where the denial of service attacks having been most common. [4] The defense industry, information technology companies, and the defense establishment team up to defend the state against these attacks, and seek to establish a broad militarized ability to hack back on the initial aggressor. [5] The growing number of attacks are frustrating, and as of today it is illegal for any private entity to hack back in the US [6] and the UK, [7] but there is a strengthened political acceptance for allowing a wider use of hacking back, [8] maybe even beyond the governmental agencies' realm. The US Congress endorsed the "Commission on the Theft of American Intellectual Property", which proposed a model for corporate hack back to enable corporations to strike back if attacked, [9] addressing the lack of governmental response to the increasing number of cyberattacks by allowing corporations to take action by themselves. Even if there have been concerns voiced from the business community, [10] the paradigm, in both commercial and government cyber security, is that hacking back is an opportunity.

II. THE RESTRAINED RED QUEEN

The first question, from a strategic standpoint, is hacking back warranted? As long as the cyberattacks are unsystematic, and of moderate complexity, these attacks pose marginal risk for the targeted nation. An alternative approach is that the targeted nation decides not to, on a routine basis, hack back, and instead utilizes the information delivered by initial attacker to the targeted nation's advantage. This article challenges the common perception that cyberattacks are per default unacceptable and dangerous, and introduces the concept of the restrained Red Queen.[11] [12]

In nature, there is a never-ending evolutionary arms race between predator and prey: the Red Queen Hypothesis.[13] [14] This model, the Restrained Red Queen, represents the targeted nation that refuses to play the evolutionary *tit-for-tat* game,[15] but instead silently and passively collects information from the cyberattacks, and in doing so changes from prey to predator. The claim in this article is that unilaterally not striking back can strategically create decisive capability instead of engaging in a never ending *tit-for-tat* set of digital interchanges with the attacker with no decisive end in sight.

Cyberattacks carry the seeds for technological development and evolution that drive the ability to go from prey to predator in future cyberwar.

The Internet has become a contested and militarized public space, where weak attribution and absence of global norms enables aggressive and adversarial nations to launch numerous cyberattacks on other countries, and their institutions. Nation states rush to create military cyber units for their defense, and views the open Internet as a national security threat[16] that has to be regulated, contained, and managed.[17] [18] The attacker is considered to be in a stronger position, based on the two unique tenets of the Internet: limited attribution and accountability.[19]

Nations address cyber defense in traditional military terms of attack, defense, and territorial defense lines. Military theory evaporates in cyber, because it does not take into account the unique cyber challenges: anonymity, lack of object permanence, and absence of measurement of effectiveness. Conventional military thinking is burdened by tradition and assumptions of its applicability in past solutions, which makes traditional military theory spurious in cyber. Instead, if the thoughts are aligned with the unique tenets of cyber, then ignoring the attacks is a viable option.

III. CYBER EVOLUTION AND ENTERPRISE PATCH MANAGEMENT

The present-day preparation for a future cyberwar assumes that the developments are a classic evolution with innovation, adaptation, and interchanges of predatory behavior where both sides in a cyber-conflict are engaged and drive each other's evolution, where at the end you have one winner. The predatory states and the targeted states are assumed to co-evolve to a higher level of cybersecurity development. This assumption has a critical flaw—the restrained cyber Red Queen that does not strike back is better positioned than the counter striking Red Queen.

The Western and industrialized world uses information security management systems that are designed according to the Plan-Do-Check-Act methodology (PDCA). [20] The PDCA-cycle originates from traditional industry quality assurance in the 1950s, and is also referred to as the Deming's cycle. [21] [22] The information security management systems (ISMS) are the overarching methodology to protect larger information systems. [23] [24] The ISMS is created to self-adjust and remove vulnerabilities over time. [25] [26]

The reach of cyberattacks has passed a point of being not only a personal threat, but increasingly a national security threat.

The density of vulnerabilities [27] matters because the greater the number of vulnerabilities in a targeted system, each patch is less effective as a countermeasure. If an attacker by the attack has exposed a vulnerability in a system with 100 vulnerabilities, the following patch and removal of the vulnerability would then have taken care of 1% of the vulnerabilities. A larger well-maintained system, such as a nation state pivotal information system, will have fewer critical and potentially system destabilizing vulnerabilities than consumer software and smartphone apps. [28] As an example, the US government increases spending on cybersecurity and the federal cybersecurity project is a multi-billion dollar enterprise.[29] In contrast, 50% of all enterprise smartphone apps have been developed without a budget to address security. [30]

National systems have fewer and less dense vulnerabilities, which allows the national IT systems to heal faster and consolidate the understanding of the vulnerabilities within the organization in a timely manner.

The more attacks that are launched on the national information systems, especially attacks that are unsystematic and of lower and moderate technical complexity, the stronger the defenses become in the targeted nation. A breach of information security, a system penetration through the firewalls and internal defensive measures, leads to an incident report and the systems then use the information to create a solution to avoid a future breach. In the industrialized world, these software and hardware solutions are custom-made for industries and government, where the residual vulnerabilities are fewer and less dense due to high cost-acceptance for maintenance, systematic approach, active penetration testing, and system overhauls.

The vulnerabilities that affect the general public and their home computers, such as viruses, malicious malware, and adware receive patches for their client machines by Internet security vendors and software vendors.

Corporations and government agencies are rapidly and uniformly working to deploy patches and software code updates to remove vulnerabilities,[31] and by doing so ensure healing of their IT-systems from similar future attacks by an adversarial state. Prolonged series of attacks would trigger incidents leading to rigorous securing of pre-existing vulnerabilities in the key information systems in the targeted society.

This article challenges the common perception that cyberattacks are per default unacceptable and dangerous, and introduces the concept of the restrained Red Queen.

If the number of residual vulnerabilities were 100 to start with, every exposed vulnerability reduces the total exposure to these vulnerabilities by 1%, and over time the reduction of these vulnerabilities reach levels where there are less vulnerabilities available for an attacker in a future cyber conflict to destabilize and impact policy in the targeted society. By absorbing these attacks as information, healing one by one the sparse number of vulnerabilities, the targeted nation state government reaches a higher level of cyber resilience, and ability to operate in a degraded environment.

Over time, the targeted nation will gain an evolutionary advantage over the aggressive nation by unilaterally restraining from counterattacks, and instead use the feedback loop generated by the attacks to its advantage by healing the systems, and at a later stage strike back decisively. A cyberattack that penetrates the firewall and defenses of the targeted system is a set of information that generates in standardized information security management system (ISMS) an incident report that leads to the creation of a solution to the vulnerability. The solution to the vulnerability is a set of customized programming that is distributed and implemented through the organization. These software updates are called patches. If the vulnerability is related to a specific software, the software vendor will use the incident information to create their commercial security update, patch, and then distribute it to their customers.[32] Therefore, in theory, one single identified attack can lead to the updating of millions of client computers and a rapid sharing and dissemination of risk information followed by mitigation on a broad scale.[33]

IV. FEEDBACK DENIAL AND REVERSAL OF PREDATORY POWER

If a targeted nation restrains from counter striking their attacker with cyberattacks, then the initial attacker is denied the feedback loop that would benefit their systems. As long as the Restrained Red Queen does not strike back, the advantage can increase.

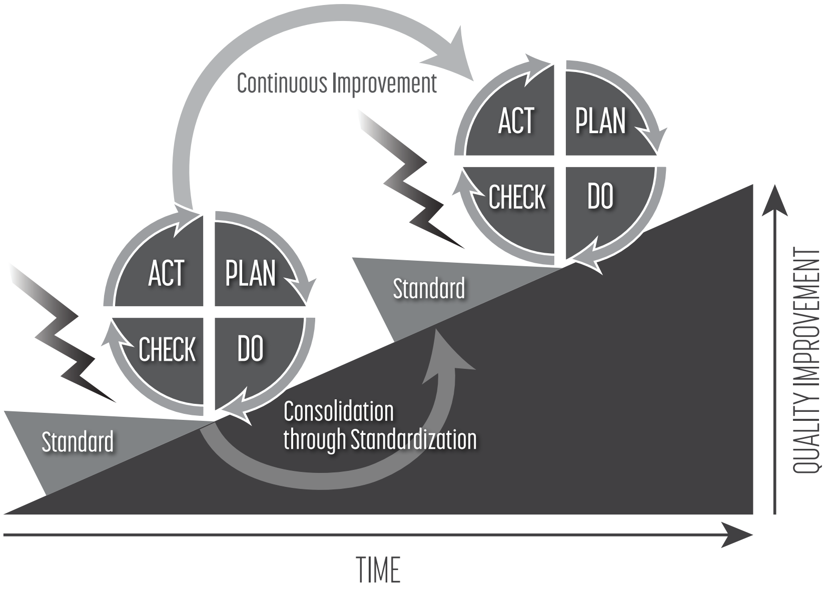

Figure 1. The cyberattacks strike the system and trigger incidents in the *Check* area in the PDCA cycle leading to continuous improvement and consolidation through standardization, which drives the targeted nation's development. Image source: Wiki Commons (modified).

Darwinism in cyberspace works elegantly—the system that is able to adapt and respond to information in the feedback loop survives. The Restrained Red Queen that refuses to strike back then will by her unilateral actions be superior at a later point in time when she decides to strike back. The Restrained Red Queen has perfected her systems and patched her vulnerabilities.

Over time, the attacking society accumulates numerous unexploited vulnerabilities that increase when new systems are added, the width of technology usage increases, and older legacy systems still exist in a mixed environment. Under attack, the restrained Red Queen facilitates software patches and vulnerability mitigation left undone by the initial attacker.

Then the Red Queen turns around utilizing automated collection of vulnerabilities against the initial attacker. A systematic automated collection of vulnerabilities can be used to scan the adversarial systems for vulnerabilities, store the vulnerabilities in an attack repository, and then launch a disproportional digital response by a massive counterstrike. The restrained Red Queen has then turned the table and prey becomes predator.

The rabbit runs faster than the fox, the rabbit survives by being faster. In cyber, any nation can be a fox if it chooses to do so, and the power of rapid digital execution increases the number of predators available in the future. In the cyber revenge of the Restrained Red Queen, the fox chases the rabbit. The rabbit becomes more of a predator the longer the fox runs and the fox is weakened. At a point in time the rabbit turns around and

Nation states operate in an environment where the systems are larger with complex structures and sparse vulnerabilities as a result of active maintenance and the pursuit strikes back with lethal power. The multitude of cyberattacks on the targeted society has trained the society, created cyber resilience, leveraged the knowledge about exploits, honed and tuned future vulnerability harvesting systems, and through these feedback loops the healed the vulnerabilities. The prey has gained a superior technical advantage and may exploit the weaknesses of the aggressor.

V. ADVERSARIES ON THE BRINK TO ENTROPY

The cyberattacks' utility is determined by the societal institutional design of the targeted nation. A targeted state that has solid and stable institutions is more resilient than a state with weak institutions and lingering entropy.[34] The current cyber engagements between nation states do not occur between states of equal or similar institutional design. China, Iran, and Russia are states where the existence of the current regime is dependent on suppression of opposition and in some cases, suppression of the popular will. The countries that are actively cyber adversarial to the United States, United Kingdom, Sweden, France, Australia, Japan, and Germany are weaker states with fragile institutions.[35] A cyber conflict is fought through the whole society,[36] within digital reach, and weak institutions and a suppressed popular will can destabilize a totalitarian regime. It is unlikely that cyber units in any of the nation states, by the cyber units' sheer size and abilities in relation to the infrastructure and size of the national economy, will have a measurable influence on the developments of a future cyber conflict. Instead, cyber defense relies primarily on already existent cybersecurity measures in the public and private sector. The main contribution the state offers is coordination and direction. Even if North Korea and Iran have designated cyber units, the units' actual influence in the event of a major counter strike is marginal, if any. The key weaknesses in the adversarial nation's cyber defenses are the lack of decentralization, initiative, and structured ways to create patches and distribute these patches due to the totalitarian institutional design of these states.

> The cyber evolution is a process where pressure from an external environment leads to natural selection and adaptation.

Therefore, the risk for a regime to become destabilized due to cyberattacks is higher in China, Iran, and Russia than in the United Kingdom or Switzerland, which are countries with very high institutional stability. For the restrained Red Queen this is important, because a counter strike does not need to be perfect to jeopardize the stability of the initial attacker. The lingering dormant entropy embedded in the weak institutional framework of the initial attacker can become a force multiplier in the counter strike.

VI. EVOLUTIONARY DENIAL

The cyber evolution is a process where pressure from an external environment leads to natural selection and adaptation. The adaptation occurs as a response to unilateral attacks. By not immediately counter striking, the targeted nation deprives the initial attacker of information that would support its ability to adapt and address its vulnerabilities. Those societal systems that are best adapted to their environment will survive, and societies that do not adapt and correct its vulnerabilities perish.[38] The adversarial predators becomes over time prey in digital Darwinism.

VII. CONCLUSIONS

The general assumptions that cyberattacks are all malicious events does acknowledge the evolutionary potential generated from cyberattacks as each attack is a set of delivered information to the target. Therefore, continuous and unsystematic attacks are important for any defender in cyber war as it first triggers the feedback loop in the PDCA driven ISMS, leading to an improvement in internal defensive measures and on a larger scale drives consolidation through standards and information sharing. The information sharing is either through direct collaboration between entities with in the same industrial group or through information system vendor based patch management that distributes the additional software needed to protect the system. On a national scale dispersed attacks over a series of targeted companies and public entities creates a national resolution to that specific software vulnerability. The attacks have then generated a leveraged cyber defense posture for the targeted state.

> If a targeted nation restrains from counter striking their attacker with cyberattacks, then the initial attacker is denied the feedback loop that would benefit their systems.

If the targeted nation refuse to engage in a *tit-for-tat* cyber conflict, but instead unilaterally holds back, the attacking state is denied the information that would trigger their cybernetic healing by the activation of their feedback loop and consolidation through standards and patch management.

Although cyberattacks within the past decade have been regarded in mass media as a monumental national security threat, they have instead generated the targeted countries' cyber-resilience by delivering vulnerability information and trigger extensive healing of the national information systems, leading to improvements instead of havoc.

The views expressed herein are those of the author and do not reflect the official policy or position of the Army Cyber Institute, the United States Military Academy, the Department of the Army, the Department of the Interior, the Department of Defense or the Department of the Interior.

NOTES

1. J. Michaels, (2013, April 21), "Pentagon expands cyber-attack capabilities," *USA Today,* Available at: http://www.usatoday.com/story/ news/nation/2013/04/21/pentagon-expanding-offensive-cyber-capabilities/2085135/.

2. E. Bumiller and T. Shanker, (2012, Oct. 11), "Panetta Warns of Dire Threat of Cyberattack on US," *New York Times.*

3. W.J. Lynn III, "Defending a New Domain: The Pentagon's Cyberstrategy," *Foreign Affairs,* September 2010, 97-108.

4. W. D. Jackson, M. Jickling, and B. Webel, "The economic impact of cyber-attacks," *Congressional Research Service,* Library of Congress, 2004, 7.

5. J. Kallberg, "A Right to Cybercounter Strikes: The Risks of Legalizing Hack Backs," *IEEE IT Professional,* pp. Jan.-Feb. 2015, 30-35.

6. 18 U.S. Code § 1030, 'Fraud and Related Activity in Connection with Computers', *United States Code,* title 18, part I, chapter 47, 1986.

7. H.M. Government, Computer Misuse Act 1990, Parliament of the United Kingdom.

8. C.M. Matthews, (2013, June 2), "Support Grows to Let Cybertheft Victims 'Hack Back," *Wall Street Journal Online.*

9. Commission on the Theft of American Intellectual Property, the *IP Commission Report,* 22 May 2013.

10. J. Westby, (2012, Nov. 12), "Caution: Active Response to Cyber Attacks Has High Risk," *Forbes,* Available: <www.forbes.com/sites/jodywestby/2012/11/29/caution-active-response-to-cyber-attacks-has-high-risk>.

11. L. Van Valen, "A New Evolutionary Law", *Evolutionary Theory* vol. 1, 1973, 1-30.

12. G. Bell, *The Masterpiece of Nature: The Evolution and Genetics of Sexuality,* Berkley, USA: University of California Press, 1982.

13. L. Van Valen, "Molecular Evolution as Predicted by Natural Selection," *Journal of Molecular Evolution* vol. 3/2, 1974, 89-101.

14. L. Van Valen, "The Red Queen," *American Naturalist,* 1977, 809-810.

15. . B. Quental, and C. R. Marshall, "How the Red Queen Drives Terrestrial Mammals to Extinction," *Science* vol. 341/6143, 2013, 290-292.

16. J. A. Lewis, "National Perceptions of Cyber Threats," *Strategic Analysis* vol. 38/4, 2014, 566-576.

17. K. B. Alexander, "Warfighting in Cyberspace," *Joint Forces Quarterly* vol. 46/3, 2007.

18. J. Kallberg, and B. Thuraisingham, "Cyber Operations Bridging from Concept to Cyber Superiority," *Joint Forces Quarterly,* vol. 68/1, 2013.

19. D. T. Fahrenkrug, "Countering the Offensive Advantage in Cyber-Space: An Integrated Defensive Strategy" in proceedings of the 4th International Conference on Cyber Conflict, NATO CCD COE Publications, Tallinn , 2012, 197-207.

20. C. Pelnekar, "Planning for and Implementing ISO 27001," *ISACA Journal,* vol. 4, 2011.

21. N. R. Senapati, "Six Sigma: Myths and Realities," *International Journal of Quality & Reliability Management,* vol. 21/6, 2004, 683-690.

22. Y. Kondo, "Emphases of Japanese Total Quality Management in the 1980s," *Total Quality Management* vol. 1/1, 1990, 23-32.

23. D. W. Straub, and R. J. Welke, "Coping with Systems Risk: Security Planning Models for Management Decision Making", *MIS Quarterly,* 1998, 441-469.

24. F. O. Sveen, J. M. Sarriegi, E. Rich, and J. J. Gonzalez, "Toward Viable Information Security Reporting Systems," *Information Management & Computer Security,* vol. 15, 2007, 408-419.

25. C. N. Johnson, "The benefits of PDCA," *Quality Progress,* vol. 35/5, 002 120.

26. R. Saint-Germain, "Information Security Management Best Practice Based on ISO/IEC 17799," *Information Management Journal* vol. 39/4, 2005, 60-66.

27. Bruce Schneider, (2014, May 19), "Should U.S. Hackers Fix Cybersecurity Holes or Exploit Them?," *The Atlantic,* Available: http://www.theatlantic.com/technology/archive/2014/05/should-hackers-fix-cybersecurity-holes-or-exploit-them/371197/.

28. S. R. Femerling, Vulnex, Available: http://media.blackhat.com/bh-eu-12/Rose/bh-eu-12-Rose-Smartphone_Apps-WP.pdf.

NOTES

29. A. Shalal and A. Slyukh, (2015, Feb. 2), "Obama seeks $14 billion to boost U.S. cybersecurity defenses," *Reuters Online,* Available: http://www.reuters.com/article/2015/02/02/us-usa-budget-cybersecurity-idUSKBN0L61WQ20150202.

30. L. Ponemon, IBM, "IBM-Sponsored Ponemon Institute Study Reveals Alarming State of Mobile Security for Apps," Available: http://securityintelligence.com/mobile-insecurity/.

31. T. Gerace, and H. Cavusoglu, "The Critical Elements of the Patch Management Process," *Communications of the ACM,* vol. 52/8, 2009, 117-121.

32. H. Cavusoglu, H. Cavusoglu, and J. Zhang, "Security Patch Management: Share the Burden or Share the Damage?," *Management Science,* vol. 54/4, 008, 657-670.

33. B. Brykczynski, and R. A. Small, "Reducing Internet-based Intrusions: Effective Security Patch Management," *IEEE Software,* vol. 20/1, 2003, 50-57.

34. J. Kallberg, B. Thuraisingham, and E. Lakomaa, "Societal Cyberwar Theory Applied: The Disruptive Power of State Actor Aggression for Public Sector Information Security", in proceedings of the IEEE EISIC European Intelligence and Security Informatics Conference, 2013, 212-215.

35. L. Chaudhary, A. Musacchio, S. Nafziger, and S. Yan, "Big BRICs, Weak Foundations: The Beginning of Public Elementary Education in Brazil, Russia, India, and China," *Explorations in Economic History* vol. 49/2, 221-240, 2012.

36. J. Kallberg, and R. A. Burk, "Cyber Defense as Environmental Protection - The Broader Potential Impact of Failed Defensive Counter Cyber Operations' in Conflict and Cooperation in Cyberspace – The Challenge to National Security in Cyberspace, Panayotis A. Yannakogeorgos and Adam B. Lowther, Eds., New York, NY: Taylor & Francis, 2013.

37. J. Kallberg, and R. A. Burk, "Failed Cyberdefense: The Environmental Consequences of Hostile Acts," *Military Review,* vol. 3, 2014, 22-25.

38. S. J. Gould, "Ever Since Darwin: Reflections in Natural History," New York, NY: WW Norton & Company, 1992.