Strategic Analysis

ISSN: 0970-0161 (Print) 1754-0054 (Online) Journal homepage: http://www.tandfonline.com/loi/rsan20

The Flaw of Immediate Cyber Counter Strikes

Jan Kallberg & Rosemary A. Burk

To cite this article: Jan Kallberg & Rosemary A. Burk (2017) The Flaw of Immediate Cyber Counter Strikes, Strategic Analysis, 41:5, 510-514, DOI: 10.1080/09700161.2017.1343265

To link to this article: http://dx.doi.org/10.1080/09700161.2017.1343265

Strategic Analysis, 2017
Vol. 41, No. 5, 510–514, https://doi.org/10.1080/09700161.2017.1343265

Commentary

The Flaw of Immediate Cyber Counter Strikes

Jan Kallberg and Rosemary A. Burk

A dominant paradigm for militarised cyber operations, owing to a growing interest in such actions, is seeking an ability to strike back and launch cyber counter attacks immediately after being attacked. This commentary challenges view based on the argument that it leads to a contra-productive tit-for-tat game with no decisive or deterrent outcome. It argues that cyber attacks are information, which an initially passive targeted society can gather to refine and consolidate its cybersecurity and over time receive an advantage over the initial attacker. Therefore, a restrained posture would be beneficial if utilised for refinement, information-gathering, development and preparing for enhanced abilities to cyber counter strike once an advantage is reached.

The Internet has become a contested and militarised public space, where weak attribution and absence of global norms have enabled aggressive and adversarial nations to launch numerous cyber attacks on other countries and their institutions. The paradigm has been following the assumption that all cyber attacks are malicious and bad. This commentary is questioning whether it is beneficial to limit cyber attacks to be generally labelled malicious, and our commentary seeks to add that cyber attacks can be valuable for the defender's cyber defence. Every cyber attack is a piece of information—even if it has no effect or fails to reach its goal. The embedded information provided by the cyberattacks can serve as guidance for cyber defence and countermeasures in cyberspace.

The massive aggregation of information provided by numerous unsystematic cyberattacks is a resource that gives the defender an ability to adapt, which is paid less attention compared to the tit-for-tat provoking pursuit of counter cyber abilities and internal defensive measures to fend off the cyber attack.

The main concern in striking back is that it also drives the adversary's evolution, and would lead to an ever-ongoing race to perfection; meanwhile, both parties affect each other's development. What happens if one party refuses to engage with the other party—and instead accumulates the information provided by the attacking party to get the strategic advantage?

If we see future cyber engagements as a form of war by itself and not a joint enabler to army, navy and air force, then cyberspace operations need to have decisive power. Decisive power is reached when an engagement either leads to the destruction

Dr. Jan Kallberg is Assistant Professor at the United States Military Academy and Research Fellow/ Research Scientist at the Army Cyber Institute at West Point (ACI), West Point, New York.
Dr. Rosemary A. Burk is a Senior Biologist with the US Fish and Wildlife Service. Washington DC.

of the enemy's resources or forces the enemy to submit to foreign will. How can cyber attacks be decisive? In our view, the attack needs to be massive, concentrated in time and destabilising. The preparation to launch a major strategic cyber campaign then requires understanding, resources, time and ability to adapt to a posture that disallows the enemy the option to utilise the same digital blunt force. The gathering of information during the restrained initial phase enables cyber evolution and development of a resilient cyber defence posture. Cyber attack abilities are then a strategic option to confront adversarial societies.

The current alternative is to unsystematically launch cyberattacks against the adversary where exploitation opportunities occur, which is likely to degrade parts of the information infrastructure, but will not reach any strategic goals. If an adversarial society is unaffected by a cyber conflict, the conflict itself has not reached a decisive outcome, and results only in a tit-for-tat game or a stalemate. How do we achieve a decisive outcome?

Strategic outcome is likely to be achieved by a massive counter strike utilising numerous zero-day vulnerabilities. For a state to reach that level of strategic dominance, from which deterrence can be derived, it would require massive information sources about potential attack vectors, time and analytic ability. The repository of vulnerabilities is created by the information retrieved from the attacks the targeted nation endures.

If the targeted nation refuses to strike back, and instead aggregates the ability to strike back later in time with decisive power, then the attacker is denied the information to drive its evolution. The rationale is the opportunity to shock the targeted society and, at the same time, avoid adaptive behaviour that mitigates the damage from the attacks. The rapid execution denies the initial attacker the opportunity to create defensive measures and evaporates any possibility to strategically lead the cyber defence.

An attack will fail to destabilise the targeted society if the institutions are intact after the attack—or able to operate in a degraded environment. Therefore, it is important to ensure that the attack is of the magnitude that forces the targeted society over the threshold to entropy.

Instead of exploiting the opportunity provided by the information generated from cyberattacks, most nation states rush to create a military cyber unit for their defence, and start to see the earlier open and liberal Internet as a national security threat that has to be regulated, contained and managed.[1] The attacker is considered to be in a stronger position, based on the unique tenets of the Internet, due to limited attribution and accountability. These developments have been driving a policy change in several countries towards an aggressive posture, utilising covert action and offensive cyber operations that enable these countries to strike back against cyber attacks. We suggest that unilaterally not striking back can strategically create decisive ability, instead of engaging in a never-ending tit-for-tat set of digital interchanges with the attacker with no decisive power or end in sight. In nature, there is a never-ending evolutionary arms race between predator and prey: the Red Queen Hypothesis. The Red Queen refers to a character in Lewis Carroll's *Through the Looking-Glass*, who remarks that in her world constant running is required to remain at the same spot. The analogy is used in evolutionary biology for explaining adaptive behaviours, where prey and predator keep adapting to each other, and the relationship between them is not changed even if they are developing. In cyberspace, it is different when the prey can be predator to achieve or learn these skills over time.[2]

The present-day preparation for a future cyber war assumes that these developments constitute a classic evolution with innovation, adaptation and interchanges of predatory behaviour where both sides in a cyber conflict are engaged and drive each other's evolution. The predatory states and the targeted states are assumed to co-evolve to a higher level of development by being exposed to external pressure.

This assumption has a critical flaw—the reluctant cyber Red Queen that does not strike back is better positioned than the counter-striking Red Queen.[3] The Western and industrialised world uses information security management systems (ISMSs) that are designed according to the plan-do-check-act (PDCA) methodology.[4] The ISMSs are the overarching methodology to protect larger information systems. The ISMSs are created to self-adjust and remove vulnerabilities over time. The more attacks are launched, especially in an unsystematic manner and of lower and moderate technical complexity, the stronger does the defence become in the targeted nation. The methodology of continuous improvement, consolidation by establishing security baselines and correction of weaknesses utilises the information from the unsystematic attacks in an efficient manner to over time significantly improve the targeted organisations' cyber resilience and cyber defences.

A breach of information security, a 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 industrialised world, these software and hardware solutions are custom-made for industries and government, and distributed to the public for their client machines by Internet security vendors such as McAfee and Symantec. Industrialised corporations and government agencies are rapid and uniform in deploying patches and software code updates to remove vulnerabilities, and by doing so ensure healing of their IT systems after similar future attacks by an adversarial nation. Prolonged series of attacks would trigger incidents that would lead to rigorous securing of pre-existing vulnerabilities in the targeted society. Targeted nations will gain an evolutionary advantage over the aggressive nation by unilaterally restraining from counter attacks, and instead can use the feedback loop generated by the attacks to their advantage, and at a later stage strike back decisively. An attack generates in a standardised ISMS an incident report that leads to the creation of a solution to the vulnerability. The solution to the vulnerability is a set of customised programming that is then distributed and implemented through the organisation. These software updates are called patches. If the vulnerability is related to a specific software, the software vendor uses the incident information to create its commercial security update patch and then distribute it to its customers. So 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 (Figure 1).

If a targeted nation restrains from counterstriking their attacker with cyber attacks, then the initial attacker is denied the feedback loop that would heal its systems. As long as the Red Queen does not strike back, the advantage can increase. Darwinism in cyberspace works elegantly—the system that is able to adapt and respond to information in the feedback loop survives. The reluctant 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 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

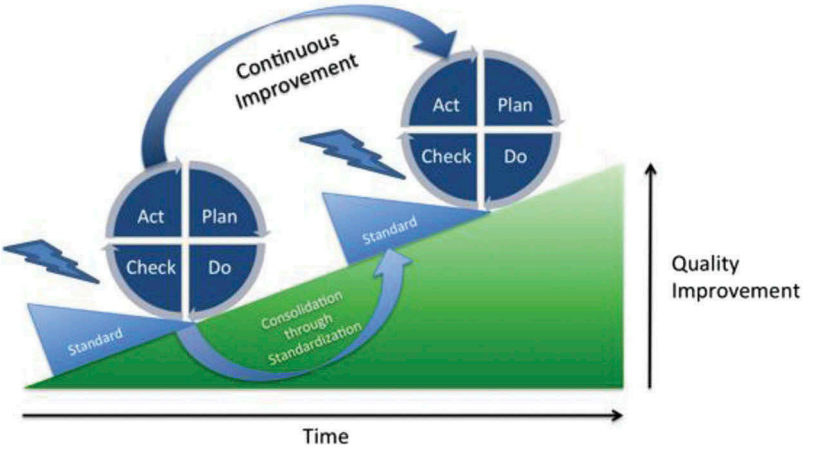

Figure 1. The cyber attacks strike the system and trigger incidents in the 'Check' area in the PDCA cycle, leading to continuous improvement and consolidation through standardisation, which drives the targeted nation's development. Image source: Wiki Commons (modified).

and older legacy systems still exist in a mixed environment. So, the work that the Red Queen, under attack, has been forced to do, such as software patches and vulnerability mitigation, is undone by the initial attacker.

Then the Red Queen turns around, utilising 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 counter strike. The reluctant Red Queen has then turned the table, and prey becomes predator.

In cyberspace, any nation can be a predator if it chooses to do so, and the power of rapid digital execution increases the number of predator actions available in the future. In the cyber revenge of the reluctant Red Queen, the predator chases the prey. The prey is continuously improving and strengthening and becomes more of a predator the longer the initial predator attacks, and the initial predator is weakened. At a point in time the transformed prey turns around and strikes back with lethal power. The multitude of cyberattacks on the targeted society, the 'prey', have trained the society, created cyber resilience, leveraged the knowledge about exploits, honed and tuned future vulnerability harvesting systems and triggered by feedback loops the healing of the vulnerabilities. The prey has gained a superior technical advantage and may exploit the weaknesses of the aggressor.

A cyber evolution is an evolutionary process as it works in nature, where pressure from an external environment leads to natural selection and adaptation. The adaptation occurs as a response to unilateral attacks. By not counterstriking, the targeted nation removes the pressure from the external environment for the initial attacker and slows down the initial attacker's ability to adapt. The initial attacker's ability to develop and have an evolution to a higher ability is slowed down due to the lowered external pressure and incentive for adaptive behaviour. According to Darwin, only those who can adapt will survive. The nation state's systems that do not adapt and correct their vulnerabilities die. The adversarial predators become over time prey in digital Darwinism. The reluctant

Red Queen will produce internal adaptation for her own and deny its attacker the feedback the attacker needs to develop to the same level to keep up with the Red Queen.

Therefore, cyberattacks, which have gained massive media attention in the last decade as a monumental national security threat, have instead secured the targeted countries' cyber-reliance because these attacks were unstructured and lacked a systematic approach, and the crude attacks provided information leading to refinement and increased resiliency. The Reluctant Red Queen concept sees cyberattacks as information, and a denial of counter-attacks is a denial of information, and information is essential for each party to heal its systems. The information landscape, which forms our opinions, is to a high degree formed by vendors, solution-providers and the defence industry, who all have significant stake in projecting the Internet, and cyberspace, as an all high-risk hostile environment with a variety of negative outcomes from cyberattacks. If there were no cyberattacks, the information needed for improvement and adaptive behaviour would not be present, and over time the risks and the vulnerabilities would increase. Cyberattacks provide the information needed for improvement. So, the question then is—are cyberattacks bad? Maybe cyberattacks are not all bad. If the information is harnessed and utilised, there are a significant number of beneficial cyberattacks—contrary to the popular view. Cyberattacks are necessary to be absorbed to perfect a cyber defence posture, and a reluctant initial position, restraining the urge to cyber counter strikes, is likely to be a long-term more viable strategic direction than seeking to reactively, and as a reflex to initial attacks, pursue immediate counter strikes.

Disclaimer

The views expressed herein are those of the authors 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 Defense, US Fish and Wildlife Service, the Department of the Interior, or the US Government.

Disclosure statement

No potential conflict of interest was reported by the author(s).

Notes

1. Keith B. Alexander, 'Warfighting in Cyberspace', *Joint Forces Quarterly*, 46(3rd quarter), 2007; Jan Kallberg and Bhavani Thuraisingham, 'Cyber Operations Bridging from Concept to Cyber Superiority', *Joint Forces Quarterly*, 68(1st quarter), 2013.
2. L. Van Valen, 'Molecular Evolution as Predicted by Natural Selection', *Journal of Molecular Evolution*, 3(2), 1974, pp. 89–101; L. Van Valen, 'The Red Queen', *American Naturalist*, 1977, pp. 809–810.
3. Detmar W. Straub and Richard J. Welke, 'Coping with Systems Risk: Security Planning Models for Management Decision Making', *MIS Quarterly*, 22(4), 1998, pp. 441–469; Finn Olav Sveen, Jose M. Sarriegi, Eliot Rich and Jose J. Gonzalez, 'Toward Viable Information Security Reporting Systems', *Information Management & Computer Security*, 15(5), 2007, pp. 408–419.
4. Charu Pelnekar, 'Planning for and Implementing ISO 27001', *ISACA Journal*, 4, 2011.