Strategic Cyberwar Theory – A Foundation for Designing Decisive Strategic Cyber Operations

Research · October 2015

DOI: 10.13140/RG.2.1.3099.7207

1 author:

Jan Kallberg
United States Military Academy West Point
60 PUBLICATIONS **96** CITATIONS

SEE PROFILE

Strategic Cyberwar Theory – A Foundation for Designing Decisive Strategic Cyber Operations

Dr. Jan Kallberg

INTRODUCTION

Each strategy has a foundation—an overarching way of explaining why things are the way we see them and how to successfully reach our goals. Therefore, strategy is theory-based because theory provides an intellectual framework for predicting outcomes leading to the end goal the strategy pursues. This article will present the strategic cyberwar theory whose utility is tied to the likelihood of institutional instability in the targeted nation. In an ideal scenario, a nation conducts systematic cyber attacks against the targeted adversary's institutions triggering the dormant entropy embedded in a nation possessing weak institutions. This will lead to submission to foreign will and intent.

This framework will the change the way nations view cyber. It is no longer an enabler for joint operations, but instead a strategic option to confront adversarial societies. The current alternative to strategic cyberwar theory is to unsystematically attack the adversary with cyber attacks where exploitation opportunities occur, which is likely to degrade parts of the information infrastructure, but will not attain any strategic goals. If an adversarial society is unaffected by a cyber conflict, the conflict itself has not reached a decisive outcome, and results in a tit-for-tat game or stalemate. Decisive outcome must lead to policy change as a partly or full submission to foreign will by the targeted society. The decisive cyber outcome is either reached by removing military capacity through cyber attacks or destabilization of the targeted society. The removal of military capacity is likely temporary, followed by software coding to close these limited vulnerabilities, compared to a societal destabilization that jeopardize the regime.

In strategic cyberwar theory, attacking the adversarial nation's institutional framework will result in destabilization. If a nation is destabilized, it can be subdued to foreign will, and the ability for the current regime to execute their strategy evaporates due

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 abilities; especially offensive cyber operations as an alternative policy option. His personal website is www.cyberdefense.com.

to loss of internal authority. The theory's predictive power is strongest when applied to targeting theocracies, authoritarian regimes, and dysfunctional experimental democracies, and their common tenet of weak institutions. [1] Fully functional democracies, on the other hand, have in cyberwar a definite advantage because advanced democracies have stable and accepted institutions. Nations openly hostile to democracies are in most cases totalitarian states that are close to entropy. The reason these totalitarian states maintain their power is through suppression of the popular will. Any removal of the pillars of suppression will destabilize the regime design and key institutions that make it functional, and could release the popular will. A destabilized and possibly imploding Iranian regime is a more tangible threat to the ruling theocratic elite than hacked military information subsystems. Dictators fear the wrath of the masses.

Strategic cyberwar theory looks beyond the actual digital interchange, the cyber tactics, and instead creates predictive power of how a decisive cyber conflict should be conducted in pursuit of national strategic goals.

The Need for Cyber Theory

Theory is an overarching way of combining ideas, phenomena, and facts, in a generalized form, to seek to explain specific outcomes. Theory's strongest tenet is predictability. Theory can serve as guidance to prepare for future events and ensure these outcomes are favorable. Theories are created to better understand the world. As an example, the democratic peace theory, [2][3] asserts that democratic states do not fight each other, and therefore the theory predicts citizens on both sides of the Saskatchewan and North Dakota border should not fear the imminent risk of a military invasion.

In a militarized Internet, it is convenient to rely on traditional military theory transposed into cyber.[4] It works as an intellectual short cut, but the traditional military thinking fails to acknowledge the unity tenets of cyber. Traditional military theory applied to cyber conflict has four challenges: anonymity, object permanence[5], measurable results, and rapid digital execution. In a Clausewitzian world, these challenges were non-existent. First, the enemy was clearly identified; a state of war was declared; a French Napoleonic general overlooking the battle could clearly distinguish a thin red line of British troops waiting for the advancing French Guards in blue uniforms. There was a basic understanding of who were the parties in the conflict, their past actions, and the strategy that drove their action. Next challenge for traditional military strategy is object permanence. The general could march its armies to a point where the next day the battle is joined with a map laying out his course of action. The landscape would be intact the next day, the roads had not moved, and the hills stood where they should. If there is no object permanence, maneuvering concepts[6] become irrelevant because maneuver increases the opportunity for success, and if we are unable to relate in time and space, maneuvering is nullified. The third challenge is quantifiable results. The French Napoleonic general storming the thin red line of British troops could see with his own eyes how the line of British troops became thinner and thinner following each rifle volley. The French general would receive an accurate measurement of effectiveness in real time, forcing a retreat if the British were still standing after the French Guards lost their battlefield thrust. Measurable results are needed as information for further decision-making and battle assessment.

If an adversarial society is unaffected by a cyber conflict, the conflict itself has not reached a decisive outcome, and results in a tit-for-tat game or stalemate.

Cyber lacks the feedback loop of quantifiable results and with no measure of effectiveness. The next move in traditional military theory relies on a chain of events leading to a decisive moment. Computers at war do not engage at human speed, the engagements occur at computational speed. Even if we solved the challenges of anonymity, the lack of object permanence and the absence of measurable results, computerized machine speed in which premeditated systematic cyber attacks would eradicate any influence of human leadership. In reality, the cyber attacks would be over before any leadership understood the strategic landscape. If the attacks were not premeditated, but relied on harvesting vulnerabilities in an ongoing conflict, the time frames in which larger future engagements could occur limits, or in worst case nullifies, the ability to orchestrate the cyber defense. The uniqueness of cyber removes the predictive power of traditional military strategy.

Going from the Unknown to the Known

If battle results cannot be quantified, there is no object permanence, and the assumed enemy is anonymous, and the battle occurs at computational speed; any grander battle strategy is becoming inferences about the unknown. Strategic cyberwar theory [7] utilizes the thinking of Bertrand Russell in his version of Occam's razor: "Whenever possible, substitute constructions out of known entities for inferences to unknown entities." [8] Occam's razor is named after the medieval philosopher and friar William of Ockham who stated that in uncertainty the fewer assumption the better and pursuing simplicity by relying on the known until simplicity could be traded for greater explanatory power. The following statements are basic knowledge with limited uncertainty.

Societies are engaged in conflicts. The cornerstone for any society is institutions. The institutional resilience varies by nation, from stable democracies to totalitarian states on the brink to entropy. The destabilization effort needed to impact the whole society must have an intensity reaching beyond the targeted nation's resiliency.

If institutions fail, society will be destabilized and weakened. A destabilized society collapses or is subdued to foreign power. These above statements are established common knowledge in political science, and act as a stated known. Following the stated known, strategic cyberwar theory seeks to explain how an adversarial society can be destabilized and subdued by a major cyber campaign. Cyberwar has to be quickly executed, shocking the targeted society, and at the same time avoid adaptive behavior that mitigates the damages from the attacks. The rapid execution denies the targeted nation the opportunity to create defensive measures and eliminate any possibility to strategically lead a coherent cyber defense.

Fully functional democracies, on the other hand, have in cyberwar a definite advantage because advanced democracies have stable and accepted institutions.

A cyber attack will fail to destabilize the targeted society if the institutions remain intact following the assault or operate in a degraded environment. Therefore it is important to ensure the cyber attack is of the magnitude that forces the targeted society over the threshold to entropy. [9]

The Future Cyberwar

Within the first two decades of the Internet, the public discourse regarding cyberwar has injected digital fear and belief that everyone is vulnerable to cyber attacks. The initial view stressed that limited options were available to prevent cyber attacks [10], generating

a cyber-Pearl Harbor hysteria,[11][12] juxtaposed with the belief that cyberwar was unlikely to happen.[13]

The positional underpinning that cyberwar is unlikely is based on the premise that its impact would not reach the threshold of war. Thomas Rid, and other proponents of this concept focus their analysis on unsystematic attacks with modest complexity. These simple intrusions exploit single digital opportunities, such as theft of data or marginal system disruptions, instead of seeking geopolitical objectives. One of Rid's main arguments is that cyberwar has never reached the Clausewitzian threshold of war. What is war in a Clausewitzian weltanschauung? According to Clausewitz, the purpose of war is to conquer and destroy the armed power of the enemy, take possession of its material and other sources of national power, and gain public approval.[14] Cyber does not want to possess, as stipulated in Clausewitz's definition, so according to the Clausewitzian definition it fails to meet the definition of war. The absence of actual casualties, or similar destruction, in cyberwar is a result of what is considered a cyberwar. A set of sporadic denial of service attacks on social media will naturally not reach the threshold for cyberwar, but destabilization of a regime utilizing cyber will subscribe to the definition of war. It is a perpetrated and intended attack on a nation state in pursuit of removing authority and control, which can in dormant entropies trigger civil war, regime collapse, and (or) violent regime shift.

The notion that cyber cannot be a tool for war itself is dated and naive. The recent entrance of state actors as heavily engaged cyber perpetrators changed the earlier cyber attack paradigm of unfunded individuals hacking into systems because they saw the opportunity to do so, and moved it to a new set of goals and intents that are aligned with the interests of the state actor.[15] The focus on the lower levels of digital interchanges has colored the debate about future cyberwar.

The international community has not witnessed a cyberwar, but instead view anecdotal digital interchanges that serve limited state interests. The Mutual Assured Destruction (MAD) theory of nuclear deterrence works well without any mutual destruction having occurred. The absence of past events does not remove the likelihood of future occurrence. If that was true—the claim that cyberwar will not happen because it has not happened—then a nuclear missile interchange would be impossible in the future because there are no past events.

Competing Cyber Strategy Thoughts

The strategic cyber discourse in recent years has a limiting central theme that cyber can only support and enable existing military and geopolitical operations. This core argument views cyber purely as an enabler for joint operations in the absence of a successful cyber-heavy conflict. The cyber theorizing paradigm refuses to acknowledge the oppor-

tunity for decisive cyber capabilities in 30 to 40 years, and instead, base their analysis on current capacities, and focus on marginal effects of unstructured, mainly simplistic, and sporadic cyber attacks. Path dependency [16][17] and tradition [18] should not blur or remove the strategic lenses in which we see the opportunity cyber brings. The risk of seeing the cyber world emerging as a mechanical part of the environment assumes that it is submerged and will not change. The trap that is created by path dependency and tradition can be presented by another word—assumption.

The main risk in the current cyber discourse focuses on cyber as purely an enabler of joint operations. This is featured in numerous assumptions, and a product of traditional burdened perceptions:

1. lacking understanding of the reversed asymmetry of the conflict, where a state can attack a domestic public entity and individual citizens,
2. the absence of object permanence,
3. the belief that cyber conflicts solely will be a match between military networks,
4. that digital interchange is conducted according to our concept of ethics and norms,
5. absence of acceptance of the rapid time frame interchanges will occur,
6. reliance of non-existent measure of effectiveness (MOE),
7. weak comprehension of the imminent future's automated computational speed conducted harvest of vulnerabilities and execution of attacks, and
8. the impact of artificial intelligence in combination with automated harvest of vulnerabilities.

If cyber warfare is limited to enabler status, other operational intent will drive the execution towards the strategic goal. Cyber capabilities offer a strategic opportunity that will grow in coming decades. Cyber effects will be limited if subordinated to enabler status, and by doing so provide democracies reduced military options.

Analogies with nuclear warfighting capabilities have striking similarities with cyber, such as both cyber and nuclear weapons share the power of projected uncertainty. According to Kenneth Waltz, it is not what you do, but instead what you can do that gives you the power. [19] Cyber and nuclear weapons both have global reach with minimal ground presence. These similarities are more shared characteristics than strategies. On the other hand, legal theories offer no direct guidance on how to fight in the cyber domain, but instead provide numerous restrictions. [20] Law is a codification of political thinking dealing with current issues, but lacks predictive theoretical power.

Cyber: Enabling Tool or a Way to Fight?

Colin S. Gray argues that cyber power is first and foremost enablers of joint military operations.[21] Secondly, Gray assert that a cyber offensive will not be lethal enough to have a major military impact. Third, cyber is information and information can be ignored. Gray's fourth conclusion is that the wide-spread fear for a stand-alone cyber Armageddon is not logical because it is unlikely to happen. Martin Libicki[22] agrees with Gray, and argues that cyber is not a stand-alone mechanism to fight a conflict, but instead an enabler, and he struggles to see cyber as anything else than attacks on computer and networks. Libicki states; "A cyber attack carried out against our military can, at worst, return it to its pre-networked condition."[23] The weakness in Libicki's argument is that he assumes cyber conflict would be a military-against-military engagement. It is reasonable to posit that Western cyber attack might be restrained, and aimed at exclusively military targets, but nothing ensures that an attack launched by a totalitarian state will obey democratic moral codes, normative ethical values, and restrains. The notion that a future cyber attack will occur in a controlled environment within the realm of old school 'fair play' is specious and generates false security.

The arguments presented by Gray and Libicki might be relevant in the snapshot of today, but these arguments are burdened by tradition, and a part of a larger time-bound context. Logically, it is likely that cyber capabilities will radically progress from this point in time.

> Cyberwar has to be quickly executed, shocking the targeted society, and at the same time avoid adaptive behavior that mitigates the damages from the attacks.

Strategic Cyberwar Theory

If nation states seek to conduct decisive cyberwar, it will not be achieved by anecdotal exploits, but instead by launching a systematic destabilizing attacks on the targeted society. In strategic cyberwar theory, the intellectual works of Dwight Waldo, a leading political scientist and theorist for over 50 years, are utilized. Waldo studied the theoretical underpinnings that maintain government institutional sustainability and stability. Strategic cyberwar theory turns these theories upside down to create entropy and destabilization. This systematic approach seeks to use institutional weaknesses, popular sentiment, and underlying opposition to the targeted government as force multipliers to the effect. Cyber targeting can induce a sense of lack of control with citizens blaming the state for failing to safe-guard the societal structure.[24][25] A nation, or any society, is organized through institutional arrangement, and this requires a set of basic functionalities to operate and ensure continued stability and functionality. Institutions make a state stable, a government sustainable and functional, even in a degraded environment.

A systematic institutional cyber attack can be visualized as the collapse of a building built with prefabricated elements, such as a parking garage, or a framework of concrete beams, pillars and decking. If pressure is distributed evenly over the construction there is no risk of collapse and the building is safe. If instead the energy is concentrated on one or a set of the bearing elements, the building will collapse. Waldo's theoretical work outlines what makes a nation state stable.[26][27] The strategic cyberwar theory turns Waldo's accepted theories upside down, so instead of upholding the functionality of the targeted society, it seeks to swiftly destabilize the state. Waldo focused his theoretical work on five factors that uphold and stabilize a society: legitimacy, authority, knowledge management, bureaucratic control, and confidence. Authority could then be external authority, by leading or in some cases suppressing a people, and internal authority within the bureaucracy and political structure.

Waldo's Five Pillars for Societal Stability

Waldo's five factors summarize the pillars of all societies and governments. If a major cyber attack can undermine these pillars, the targeted state is weakened and risks implosion. Legitimate government must be legally legitimized, and capable of delivering the 'good society' or in a dictatorship 'acceptable society'. Legitimacy is a sliding grey-scale and cannot be seen as a value that the society either has or not.[28] Authority is the ability to implement policy, and in a democracy, it requires the rational acceptance of people, expectations of public good, ethics, and institutional contexts. Institutional knowledge is the ability to arrange and utilize awareness and expertise within the bureaucracy since coordination is always the major challenge. Control is the ability to dominate and have authority over a bureaucracy. Confidence is the trust people have that government delivers the expected benefits and removes that fear of an uncertain future.

These five factors are the framework that hold a government together. If depleted or removed, the absence of the factors will mortally wound a government. In strategic cyber warfare it is pivotal to attack and eliminate one or all of these pillars, which will lead to the collapse or serious damage of the targeted state.

A. Legitimacy

Legitimacy concerns not who can lead but who can govern. Waldo believed that citizens need faith in government; for government to have legitimacy, they must promise and then deliver a better life for its citizens. For a major cyber-attack seeking to damage state legitimacy, it has to darken the future for the population, and create an assumption that the leadership is unable to govern the country.

B. Authority

Authority in totalitarian regimes can be summarized as acceptance for the moment.

Authority and hierarchy are linked when the structure determines the jurisdiction of a specific position. If there is no hierarchy, there is no leadership that can be held accountable for its actions; with no accountability, any organization could fall into entropy and anarchy.

C. Institutional Knowledge

One of the major challenges for modern government is knowledge management. If public administrators are unable to organize knowledge and information, the citizens are left with the impression the government is incompetent. This is an indirect challenge to authority and could lead to societal entropy. The modern society generates overwhelming amounts of information at all levels, with much of it available over the last two decades. Knowledge is generated by agencies and the public sector through documents, actions, inquiries, publications, and policies. The increase of knowledge requires specialization, according to Waldo, but with specialization comes the challenge to coordinate the information. If a lack of knowledge and coordination affects citizens, it undermines their perception of how well government is working. Cyber attacks on institutional knowledge management will cripple the bureaucracy and anger the population.

The international community has not witnessed a cyber-war, but instead view anecdotal digital interchanges that serve limited state interests.

D. Bureaucratic Control

Complex organizations have challenges with a growing bureaucracy. Control can also be lost due to the ineffective coordination among agencies, local and state governments, and other stakeholders. When a government does not have proper bureaucratic control across organizations, jurisdiction is lost. As bureaucracy expands, so do the control issues since control requires coordination. Control issues also arise through unintentional errors. If control is lost, corruption, favoritism, public theft, and popular discontent will follow.

E. Confidence

Waldo asserted that when people feel secure, they have confidence, and are optimistic about the future; they trust government will provide necessary support. Confidence for Waldo was trust in government to deliver the society it promised. Confidence means the future is perceived to be brighter than the past; legitimacy and authority is defined in the present, confidence is forward-looking. Current global events of scarcity and competition for public resources is harmful to confidence in government, because it challenges future ability to serve citizens. Signs of systematic failure will harm the citizenry's ability to maintain confidence in government.

Examples of Targeting

Strategic cyberwar theory predicts the weaknesses of targeted governments, and assists in remotely initiated regime shift or submission to foreign power. These weaknesses are identified in each society based on the societal characteristics and tenets. Once the weaknesses are identified they are aligned with the theory and operationalized to targeting. The attack in these sectors is likely unexpected by the targeted nation, its cyber defense is defending other sectors of the society, and will initially create turmoil and confusion. These targets selected by strategic cyberwar theory differ in several cases from the traditionally prioritized assets for national cyber security and information assurance, such as military, defense-industrial, diplomatic, and executive information assets.

The actual legality of the proposed targets according to international humanitarian law is not discussed in this paper. Theories create models and seek to predict outcomes. It is up to the users, the policy creator, to align the actions the theory supports with other conflicting interests such as legal compliance, ethics, and humanitarian concerns.

Two model states are created as a visualization of cyber targeting in the pursuit of destabilization.

First - adversarial theocracy

EXAMPLE OF TARGETING MATRIX - ADVERSARIAL THEOCRACY	
Waldo's Five Factors	**Example of Targets**
Legitimacy	Legislature Revelation of Undisclosed Information Leaking Email and Communication Traffic from Top Echelon
Authority	Law Enforcement Information Systems Acquire of Loyalist Informers' Personal Data Inject Forbidden Material in Trusted Loyalists' Computers and Networks
Institutional Knowledge	Real-Estate/Cadastral Data Corrupting Land Ownership Information
Control	Destruction of Hard-Core Auxiliary Security Unit's Information Systems Destabilization of Financial Systems by Massive Pay-Outs of Public Funds
Confidence	Government Salary Systems Public Financial Support Transfers Real-Estate/Cadastral Data Corrupting Land Ownership Information

In a theocracy, leaders maintain societal stability and order with auxiliary police, and by utilizing government jobs as a tool to transfer funds to loyalists. The population's main asset is real-estate due to the lack of other financial opportunities, and the hidden secrets of the elite contradict their own public standards.

Life in the theocracy can be unpleasant, but it is stable, and if you are loyal to the regime you get a share of state income. The non-loyalist can maintain their wealth through real-estate ownership, which is their main private asset. By identifying this fabric through strategic cyberwar theory a swift and premeditated wave of cyber-attacks could destabilize the society.

As an example, theocratic Iran with private ownership of real estate assets, but with limited venues to gain wealth has an embedded vulnerability. Iran is well aware that it will be targeted in a cyber conflict, and has hardened military and critical infrastructure computer systems. The strategic cyberwar theory will identify the cadastral survey data as vulnerability based on the importance as institutional knowledge and confidence.

Cyber targeting can induce a sense of lack of control with citizens blaming the state for failing to safe-guard the societal structure.

Iran's real-estate represents the bulk of privately held assets, and tampering with cadastral data will jeopardize the popular confidence in the government. A successful attack on Iranian land survey data, creating confusion regarding who owns what, and what information to trust, can create far more societal entropy and risk for regime changing violence, than attacks degrading the Iranian Revolutionary Guard information systems. The entropy from a collapse in the cadastral and land survey systems can heavily influence societal stability. If the magnitude is multiplied by other niche targets belonging to the fabric that keeps the nation calm, the theocratic regime can fall.

The second example is a one party dictatorship that has successfully survived by providing consumption and financial reward to the crucial part of its citizenry. The one party dictatorship has a set of unique tenets with the government highly centralized and dictatorial. The building sector and real-estate is where money is funneled through informal banking institutions, which operate outside of the party-controlled system, with money providing mortgages.[29] The informal banking sector is an inviting target of opportunity.[30] All banks have a database that sorts out who owes what to who, while establishing demand. The database can be destroyed or corrupted with bold and swift systematic attacks of the informal banking system, which will unleash entropy. As in the theocracy, the one party dictatorship relies on pay-outs to loyalists, which then becomes a target with corrupted payments.

EXAMPLE OF TARGETING MATRIX - ADVERSARIAL ONE PARTY DICTATORSHIP	
Waldo's Five Factors	**Example of Targets**
Legitimacy	Deny Electricity for Iconic Administrative Centers
Authority	National Police Information Sharing Dissemination of Loyalist Informers' Personal Data
Institutional Knowledge	Real-Estate/Cadastral Data Corrupting Land Ownership Information Destruction of Permit Databases
Control	Corruption of Government Salary Pay-Outs Degrade the Blocking Operations that Prevent Access to the Complete Internet
Confidence	Informal Banking Institutions

Remotely Launched Societal Destabilization

For the attacker, the keys to successful implementation of strategic cyberwar theory is the pre-planning and mapping of the institutional design and weaknesses of the targeted society. Cyber conflict from a strategic level is a pointless exercise unless the cyber attacks influence and degrades the targeted society. The presented theory is designed to guide the development of offensive cyber operations in a strategic cyberwar between nation states.

The speed of strategic cyberwar theory negates the adaptive behavior in the targeted state. Western nations have a corporate and federal culture of rapid patch management, following the different information security management structures and protocols in place, but the potential adversarial nations have less capacity to patch their networks in time.

Rapid cyber attack ensures the feedback loop generated by the attack does not generate a system recovery. Existing patch management is too unstructured, driven by commands instead of delegated initiative, and therefore lacks rapid response mechanism.

Today, the adversarial nations' cyber security is managed by each agency and department independently without any over-arching strategic coordination. This absence of national coordination in these countries creates an opportunity to be exploited by strategic cyberwar theory with a systematic attack.

There are moral constraints and issues impacting the utilization of the theory to its full extent, such as the humanitarian responsibility for triggering civil war by remote control, and the contrary argument if the prolonged suffering under a ruthless regime would require humanitarian intervention, but that is a different debate.

The strategic cyberwar theory seeks to explain, put in context, and guide by providing a thought model with predictive power. This theory is not tied to today's policy; only 30 years ago, the fax machine was high tech. We cannot focus on current cyber capabilities, but instead, we need to think where cyber development is going and how it will transform societies in the future. It might be valuable to remember that the Wright Brothers first flight lasted 12 seconds and covered just 100 feet, but aviation did not wither away because the first flight was not transatlantic. In cyber, things will fall in place and new technology emerge, which increase the need to put cyber in a strategic context.

Conclusion

The proposed strategic cyberwar theory is a work in progress, but the claims are maturing. The core assertion is that cyber will be a means to attain geopolitical goals in the future by destabilizing adversarial nations. Strategic cyberwar theory is a tool to exploit weaknesses in adversarial states. Eventually, cyber capabilities will drive adversarial countries into entropy by creating a system shock to the institutional framework holding these countries together. As stated, traditional military theory applied to cyber conflict with four challenges: anonymity, object permanence, measurable results, and rapid execution. In a Westphalian and Clausewitzian geopolitical world these challenges were non-existent. The lack of object permanence nullifies maneuver, which until now has been essential in military strategy, and it replaces object permanence with a rapidly evolving kaleidoscope of nodes and bits. The massive anonymity in digital interchanges removes the ability to clearly understand who is your enemy, and based on that assessment gauge their abilities. Finally, with no measurement of effectiveness a fighting nation is unaware of the actual impact of the interchanges in tactical time frames and the rapid execution is likely to create a battle of which only the machines are fully aware. These four unique cyber tenets evaporate the opportunity to use traditional military thinking in cyber. If traditional military thinking is utilized to formulate a strategy, it is likely that the result would aggregate spurious assumptions and remove the opportunity for decisive offensive cyber operations as a geopolitical toolset.

Strategic cyberwar theory predicts the weaknesses of targeted governments, and assists in remotely initiated regime shift or submission to foreign power.

Strategic cyberwar theory views the adversarial nation as a framework of institutional arrangements instead of a set of military assets and digital networks. The institutional frameworks are likely to be less well defended as the industrial-military complex, but when destabilized these frameworks remove the underpinnings of the adversarial regime leading to a decisive climax to the cyber conflict. The theory also argues that attacks have to occur within a limited time frame to ensure system shock in the targeted society.

Strategic cyber war theory addresses the unique tenets of the cyber domain: anonymity, object permanence, measurable results, and rapid execution. The theory avoids the need to identify the enemy, rely on maneuvering and object permanence, require measurable tactical results, and be independent of need for actionable leadership under conflict. The strategic cyberwar theory provides a way to create a decisive strategy for nation state conflicts.

NOTES

1 Paul Brooker, *Non-Democratic Regimes: Theory, Government and Politics* (New York: Palgrave Macmillan 1994).

2 Bruce, Russett, and Maoz Zeev, 'Normative and Structural Causes of Democratic Peace', *American Political Science Review* 87 3 (1993), 624-638.

3 Bruce Russett, *Grasping the Democratic Peace: Principles for a Post-Cold War World* (Princeton: Princeton University Press 1993).

4 Thomas Rid, *Cyber War Will Not Take Place,* (Oxford: Oxford University Press 2013).

5 Jan Kallberg and Bhavani Thuraisingham, 'Cyber Operations: Bridging from Concept to Cyber Superiority', *Joint Forces Quarterly* 68 (2013).

6 Applegate, Scott D, 'The Principle of Maneuver in Cyber Operations', In Cyber Conflict (CYCON), 2012 4th International Conference on, 1-13. IEEE, 2012.

7 Jan Kallberg, Bhavani Thuraisingham, and Erik Lakomaa, 2013, 'Societal Cyberwar Theory Applied the Disruptive Power of State Actor Aggression for Public Sector Information Security', Presented at and published in *Proceedings from the 2013 IEEE European Intelligence and Security Informatics Conference* (EISIC 2013).

8 John Shand, *Philosophy and Philosophers: An Introduction to Western Philosophy,* (Montreal: McGill-Queen's Press-MQUP 2002).

9 Jan Kallberg, and Adam B. Lowther, 'The return of Dr. Strangelove', *The Diplomat,* August 20, 2012.

10 William H. Webster, Frank J. Cilluffo, and S. Lanz, *Cybercrime Cyberterrorism Cyberwarfare: Averting an Electronic Waterloo* (Washington DC: Center for Strategic & International Studies 1998).

11 Ariana Eunjung Cha, 'For Clarke, a Career of Expecting the Worst: Newly Appointed Cyberspace Security Czar Aims to Prevent Digital Pearl Harbor', *Washington Post,* Nov. 4, 2001.

12 Alison Mitchell, 'To Forestall a 'Digital Pearl Harbor,' U.S. Looks to System Separate From Internet', *New York Times,* November 17, 2001, <http://www.nytimes.com/2001/11/17/technology/17INTE.html>

13 Thomas Rid, 'Cyber War Will Not Take Place', *Journal of Strategic Studies* 35 1 (2012), 5-32.

14 Hans Wilhelm Gatzke, ed, Carl von Clausewitz: *Principles of War,* (New York: Military service publishing company 1942).

15 Jan Kallberg, and Bhavani Thuraisingham, 'Cyber Terrorism to State Actors' Covert Cyber Operations in *Strategic Intelligence Management: National Security Imperatives and Information and Communications Technologies',* Babak Akhgar and Simeon Yates, eds. (Oxford: Butterworth-Heinemann 2013).

16 Paul Pierson, 'Increasing Returns, Path Dependence, and the Study of Politics', *American Political Science Review* (2000), 251-267.

17 Paul Pierson, *Politics in time: History, institutions, and social analysis,* (Princeton: Princeton University Press 2004).

18 Heinz Guderian, Panzer Leader (New York: Dutton 1952).

19 Kenneth N. Waltz, 'Nuclear Myths and Political Realities', *American Political Science Review.* -- (September 1990), 731-745.

20 Schmitt, Michael N. ed, *Tallinn manual on the international law applicable to cyber warfare* (Cambridge: Cambridge University Press 2013).

21 Colin S. Gray, *Making Strategic Sense of Cyber Power: Why the Sky is Not Falling* (Carlisle: U.S. Army War College – Strategic Studies Institute 2013).

22 Libicki, Martin C., 'Why Cyber War Will Not and Should Not Have Its Grand Strategist', *Strategic Studies Quarterly,* (2014, Spring).

23 Libicki, 'Why cyber war will not and should not have its grand strategist', 29.

NOTES

24 Jan Kallberg, and Rosemary 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.* P. A. Yannakogeorgos and A. B. Lowther, Eds, (New York: Taylor & Francis 2013).

25 Jan Kallberg, and Rosemary A. Burk, 'Failed cyberdefense: The Environmental Consequences of Hostile Acts, *Military Review.* (May-Jun. 2014), 22-25.

26 Dwight Waldo, *The Administrative State,* (New York: Holmes & Meier Publishers 1948)

27 Dwight Waldo, *The Enterprise of Public Administration* (Novato: Chandler & Sharp 1980).

28 Jürgen Habermas, *Legitimation Crisis* (Boston: Beacon Press 1975).

29 Kellee S. Tsai, *Back-alley banking: Private entrepreneurs in China* (Ithaca: Cornell University Press 2004).

30 The Economist, 'Shadow banking in China - The Wenzhou experiment', April 7, 2012, http://www.economist.com/node/21552228>