Societal Cyberwar Theory Applied

The Disruptive Power of State Actor Aggression for Public Sector Information Security

Jan Kallberg and Bhavani Thuraisingham
CSI, Erik Jonsson School of Engineering and Computer Science, The University of Texas at Dallas
Richardson, TX 75083-0688
jkallberg@utdallas.edu

Erik Lakomaa
Institute for Economic and Business History Research
Stockholm School of Economics
Stockholm, Sweden
erik.lakomaa@hhs.se

Abstract – The modern welfare state faces significant challenges to be able to sustain a systematic cyber conflict that pursues the institutional destabilization of the targeted state. Cyber defense in these advanced democracies are limited, unstructured, and focused on anecdotal cyber interchanges of marginal geopolitical value. The factual reach of government activities once a conflict is initiated is likely to be miniscule. Therefore the information security activities, and assessments leading to cyberdefense efforts, have to be strategically pre-event coordinated within the state. This coordination should be following a framework that ensures institutional stability, public trust, and limit challenges to the state. We present a case to use societal cyberwar theory to create a national cyber defense in an event of facing a massive state actor initiated automated systematic cyber attacks to prevent a societal system shock. Societal cyberwar theory utilizes a theoretical framework created by political scientist Dwight Waldo for government stability, turns it upside down, and uses the theory to identify cyber targets and aim points. According to societal cyberwar theory the aim points to be targeted by an automated premeditated systematic attack that will cripple the targeted nation is the five pillars that upholds the state – legitimacy, authority, knowledge, control, and confidence. The failure to protect the institutional stability could undermine the state's ability to avoid submission to foreign power.

Keywords - cyber operations; cyberdefense; information assurance; offensive cyber operations; defense; cyberwar; information operations; societal cyberwar theory

I. INTRODUCTION

The recent development towards offensive cyber operations lack feasible theories how offensive cyber conflicts should be conducted. In the same way as offensive cyber operations lack feasible theoretical underpinnings it is also a gap in the theoretical foundation for cyber defense. Cyber conflict is between nation states and follows the rationale of state interests. The international community has not yet seen a cyberwar, but instead mainly anecdotal digital interchanges that serve a limited, if any, purpose to gain strategic and geopolitical state interests. The anecdotal interchanges will over time be coordinated and aligned with a systematic approach as the militarization of the Internet continues. The states will be fighting a cyberwar with the intent to seriously damage and cripple the adversarial and targeted state – or gain significant advantages in a critical juncture. A state seeking to gain an advantage is likely to seek tangible effects in near time that will cripple the targeted nation. Cyber espionage and industrial intellectual property theft seek to gain information to be utilized at a later stage, but it is not cyberwar.

Societal cyberwar theory seeks to explain how a society can be severely destabilized and crippled by a major cyber campaign. If states will conduct cyberwar it is likely not a few anecdotal exploits, but instead systematic destabilizing attacks on the targeted government. The systematic approach seeks to use institutional weaknesses, popular sentiment, and underlying opposition to the targeted government as force multipliers to the effect.

II. THE ABSENSE OF CREDIBLE CYBER DEFENSE

The launched cyber attacks the last decades have lacked a systematic design to destabilize an adversarial society. These attacks have been driven by the exploit of single digital opportunities instead of seeking gaining political and geopolitical goals. The inability to see the clash of societal systems and instead focus on the lower levels of abstraction has derailed in some cases the debate about future cyberwar [1].

One finding, and therefore an assumption, proposed in this paper is that a cyberwar has to be quickly executed [2] and unprecedented in the aim of the attack [3]. The reason is the opportunity to shock the targeted society and in the same moment avoid adaptive behavior that mitigates the damages from the attacks. A cyber conflict will then be highly automated and be executed according to preset aim points and identified vulnerabilities that are exploited on a broad scale under a short time frame. The actual acquisition of the selected vulnerabilities that are targeted could be done over years and be stored in a repository that are regularly updated similar to electronic target folders maintained by air forces. Targeting data can be automatically acquired, updated, and maintained. Advanced vulnerabilities can be acquired by sensitive intelligence and reconnaissance. A massive attack will not destabilize the targeted society if the institutions are intact after the attack – or able to operate in a degraded environment.

III. THE REACH OF GOVERNMENT

Several advanced democracies, and their ministries of defense, are creating what they define as cyber warfare capabilities. The question is if these fairly small military cyber defense units will have an impact in a cyber conflict as these units are to a high degree forensic team seeking attribution and determine vulnerabilities at a limited number of systems and

points of entry. It is unlikely that any of the cyber units, by their sheer size and abilities in relation to the infrastructure and economy, will have a measurable influence on the developments of a future cyber conflict. Instead the cyber defense in advanced democratic welfare countries relies primarily on already existent cyber security measures in the public and private sector. The main contribution that the state can offer is coordination and direction. By utilizing societal cyberwar theory weaknesses can be identified and the state can coordinate the efforts - in the pursuit of a far more adaptive and self-healing information security posture.

IV. Societal Cyberwar Theory

The ability to severely destabilize an adversarial nation through cyber attacks lies in the systematic approach that is the foundation for societal cyberwar theory. Societal cyberwar theory can destabilize a targeted state if the targeted aim points in society are systematically identified and exploited.

The lack of systematic thinking in a cyber aggressor's strategy has evaporated the opportunity for success by major state actors' offensive cyber formations – but over time the lack of systematic thinking will be solved as the militarized and contested Internet matures.

A nation, or any political structure, is organized through institutional arrangement. These arrangements require a set of basal functionalities to operate within the institution to ensure the continued stability and functionality. In political science and public administration science a significant body of literature and research has formulated what makes a state stable, a government sustainable, and institutions functional even in a degraded environment. Each country is unique in its institutional arrangements and the societal importance of these arrangements.

Societal cyberwar theory seeks to explain how a society can be destabilized and crippled by a cyber campaign to reach institutional entropy.

Systematic institutional attack can be visualized as the collapse of a building built with prefabricated elements on a framework of concrete beams, pillars and decking. If pressure is distributed evenly over the construction there is no risk for a collapse. The building is safe. If instead the energy is concentrated on one or a set of elements of the building it will collapse.

The theory is constructed by using Dwight Waldo's theoretical work seeking to explain what makes a nation state stable [6]. The societal cyberwar theory turns Waldo's highly accepted theories upside down, so instead of upholding the functionality of the targeted society it seeks to swiftly destabilize the targeted society. Waldo focused his theoretical work and scholarly productions on factors that uphold and stabilize a society and was a leading political scientist and theorist for over 50 years. These works were published in his books "The Administrative State" [4] and "The Enterprise of Public Administration" [5]. Waldo named five factors – legitimacy, authority, knowledge management, bureaucratic control, and confidence [6]. Authority could then be external authority, by leading or in some cases suppressing a people, and internal authority within the bureaucracy and political structure. If future cyber attacks target key institutional arrangements the attack can trigger effects that are in size and societal impact equal or beyond the impact of traditional kinetic warfare.

V. Waldo's Five Factors

Waldo's five factors summarize the pillars of any society and government. If a major automated attack can undermine these pillars the targeted society are either weakened or at serious jeopardy to lose its power. Legitimacy includes not only that the government is legally legitimized but capable and focused on an intention to deliver the "good society." Legitimacy is a sliding grey-scale [7] and cannot be seen as a value that the society either has or not. Authority is the ability to implement policy. In a democracy it requires the acceptance of the people based on rationalism, expectations of public good, ethics, and institutional contexts. Knowledge is institutional knowledge, the ability to arrange and utilize knowledge within the bureaucracy since coordination is the major challenge in knowledge management. Control is the ability to control what we want to control in the bureaucracy. Confidence is trust people have that government delivers the expected benefits and the removal of fear for the future. According to Waldo, feelings of vulnerability and fear of future events are the absence of confidence in government.

These five factors are the framework that holds a government together. If depleted and removed the absence of the factors will disintegrate government. In strategic cyber warfare it is pivotal to remove any of these pillars, leading to the collapse of the other, and damage the targeted society.

A. Legitimacy

Legitimacy concerns not who can lead but who can govern. Waldo believed that we need faith in government; for government to have a strong legitimacy it has to project, deliver, and promise that life would be better for citizens. For advanced welfare democracies, Waldo raised the question that if the central glue that holds society together is the expectation of more, what does that lead to? Waldo meant that if we build our society around a government that always delivers more services, benefits, and progress, what would happen if there were less of everything in the future? Scarcity of resources, and extreme austerity, would trigger challenges to the legitimacy of a regime. The recent violent and vocal reactions in Greece against severe government austerity measure are examples of these challenges to legitimacy.

In a democracy the voter need a sense that they are represented, government works for their best, and government improves life for citizens and voters. Increasing complexity and distance from the population play a role in politics and decrease legitimacy; the population is losing the sense that these political actions are in the interest of the people. In the "Administrative State", Waldo defined his vision of the "good life" as the best possible life for the population that can be achieved based on the time, technology, and resources.

For a major automated attack seeking to damage legitimacy in a welfare state it has to darken the future for the

population, create a notion that the leadership are unable to govern the country to a better position for the individual and that the current regime create undue burdens for the citizens.

B. Authority

In a democracy, authority is the ability to implement policy with the acceptance of the people based on rationalism, expectations of public good, ethics, and institutional contexts. Authority in totalitarian regimes can be summarized as acceptance for the moment. Authority and hierarchy are linked when the structure of the hierarchy determines the authority 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 would fall into entropy and anarchy.

C. Institutional Knowledge

One of the major challenges for government is knowledge management. If public administrators are unable to organize knowledge and information, the public is left with the impression that the government is incompetent. This is a indirect challenge to authority and could lead to societal entropy.

The welfare state, compared to totalitarian states, is more vulnerable as it administrates welfare programs that have to be tracking eligibility, rights and liabilities, and payments to millions of individuals. The welfare state is based on the ongoing and stable approval of the people. The totalitarian state has the option to execute violence against its population to suppress the opinion and the sentiment. In the advanced democratic welfare state failures are directly discussed and popular sentiment can shift quickly.

Knowledge is a factor that receives less attention than authority and legitimacy. Political systems are legal constructs so questions of legitimacy and authority are central to the debate; they are the foundations for government. An information society generates massive amounts of information at all levels. Increased complexity is driven by higher degrees of specialization, growing numbers of governing laws and compliance considerations, and increased diversity in society. Diversity is not only ethnic but also education, language, net maturity, and socio-economic factors. The abundance of information available within the last few decades is overwhelming and decreases public administrators' abilities to take action when needed and make wise decisions.

According to Waldo: "It might seem peculiar if not contradictory to allege a knowledge problem in a situation that has to be said to be characterized by a knowledge explosion. But the explosion of knowledge creates its own problem. The increase of knowledge demands specialization, but specialization increases the problem, with coordination – microlevel to macrolevel. How can it be put together? Who can put it together, using what principle of legitimacy-authority? Moreover, while knowledge increases overall, it increases unevenly and not necessarily in proportion to need."

Knowledge is generated by agencies and the public sector through documents, actions, inquiries, publications, and policies. All of these knowledge sources are overwhelming if not structured and organized. The increase of knowledge requires specialization, according to Waldo, but with specialization comes the problem of how to coordinate the information. To be able to organize properly the knowledge generated, specialization requires better trained public administrators. Waldo also pointed out that knowledge increases unevenly, not in proportion to need. Waldo's comment was that the public sector generates more knowledge in some sectors beyond what is needed. In other sectors with an imminent need for increased knowledge, not enough knowledge is created. This uneven creation of knowledge undermines effective government. If a lack of knowledge and coordination affects citizens, it undermines their perception of how well government is working. Cyberattacks on institutional knowledge management will cripple the bureaucracy and anger the population.

As an example to illustrate targeting, a hypothetical targeted state is a state with private ownership of assets. The targeted state is well-aware of that it could be targeted in a cyber conflict and has hardened and tested all military and critical infrastructure computer systems. The societal cyberwar theory will identify the cadastral survey data as vulnerability based on the importance as institutional knowledge and as real estate represents the bulk of the assets that are in private hands. An successful attack on the land survey data in the targeted country, creating confusion who owns what, and what information to trust, can create far more societal entropy and risk for regime changing violence, than attacks on military information systems. The entropy from a collapse in the cadastral and land survey systems can influence the societal stability heavily in a state, such as Sweden, due to the fractional equity the citizens have outside of their real estate holdings.

D. Bureaucratic Control

Complex organizations have problems with bureaucracy as they grow in size and complexity. Control can also be lost because of a lack of coordination among federal agencies, local and state governments, and other stakeholders. When government does not have 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. The widening of the public sector with increased interactivity between agencies and data sharing also increases the risk for errors.

E. Confidence

Waldo connected the words secure and confidence when he described his confidence problem. When people feel secure, they have confidence and are optimistic about the future; they trust government will provide support. Confidence for Dwight Waldo was trust in government to deliver the good society it promised. Confidence means that the future is perceived to be brighter than the past; legitimacy and authority is defined in the present, confidence is forward looking. Confidence becomes crucial especially for democracies. Emerging 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 and projected inability will harm the citizenry's ability to maintain confidence in government.

VI. Targeting Matrix

Societal cyberwar theory predicts the weaknesses of the targeted government – in the pursuit of 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.

As an example a targeting matrix will translate the five Waldo's factors to variables that are matched by targeting areas. Next step is to drill it further down to cyber tactics and aim points.

TABLE I
TARGETING MATRIX EXAMPLE

Waldo's Five Factors	Example of Targets
Legitimacy	Legislature Welfare benefits Classified information
Authority	Law enforcement Local government
Knowledge Management	Cadastral data Tax collection
Control	Air-traffic control Railways
Confidence	Energy providers Retirement funds Public financial support transfers

These targets selected by societal cyberwar theory differ in several cases from the traditional prioritized assets for national cyber security and information assurance. The absence of strategic thinking in information assurance research and education is a societal vulnerability [8].

VII. Designing Cyber Security Accordingly

Today the cyber security work is done by each agency and department independently without any strategic coordination. This lack of national coordination create and opportunity that can be exploited by societal cyberwar theory. Even if a state has a declared cyber defense strategy, it requires a process to identify potential assets, systematic vulnerabilities, institutional pivots, and assess the societal stability. As of today we have not seen any work that covers these full spectrum cyber defense dimensions.

VIII. Cyberwar and Cyber Deterrence

The key to success for implementation and use of societal cyberwar theory is the pre-planning and mapping of the institutional design and weaknesses of the future targeted society. The theory is applied after studies of the society so the theoretical framework will predict outcomes of actions and likelihood of rapid entropy and disintegration of the targeted government and nation state.

If a cyberwar is thought the strategic goal has to be to force the targeted nation to submit to foreign will and make policy changes and accept commitments that the defending nation was not accepting initially.

Cyberwar can be fought decisively if major automated attack is launched following a targeting list created using societal cyberwar theory. This war can be launched with little or short notice with devastating effect on the targeted society. The prepositioned combination of societal war theory and major automated attack has a deterring effect on any society that is confrontational. Deterrence leads to policy change and unwillingness to take action based on the potential consequences and embedded uncertainty.

The combination of societal cyber war theory and major automated attack creates significant uncertainty in the targeted society in the preamble to the actual digital exchange. The political theorist Kenneth N Waltz [9] said about nuclear arms that the power of nuclear weapons is not what you do – but instead what you could do. The combined major automated attack and societal cyberwar theory have identical tenets. The power is in what you can do and the embedded uncertainty for the enemy. Traditionally, a matured and advanced democracy is considered to have strong institutions, a higher resilience in the governmental institutions, and a greater embedded trust in the leadership. The question is if that is true under normal and controlled conditions – and if these assumptions survive societal stress and institutional disintegration as the advanced democratic welfare state has limited control over popular sentiments and individual actions. The presented theory is designed to serve as guidance to the development of offensive cyber operations in a strategic cyberwar between nation states.

References

[1] T. Rid, "Cyber War Will Not Take Place," Journal of Strategic Studies, vol. 35, no. 1, 2012.

[2] J. Kallberg and A. Lowther, "The Return of Dr. Strangelove," The Diplomat. Aug. 20, 2012. http://works.bepress.com/jan_kallberg/5/

[3] J. Kallberg, "Designer Satellite Collissions from Covert Cyberwar," Strategic Studies Quarterly, Spring 2012.

[4] D. Waldo, *The administrative state*. New York: Homles & Meier Publishers, (1948) 1984.

[5] D. Waldo, *The enterprise of public administration*. Novato: Chandler & Sharp, 1980.

[6] J. Kallberg, *The Internet as a proxy for democratic accountability and transparency---a comparative test of Waldo's five problem areas in five advanced democratic societies.* Disseration. Richardson: The University of Texas at Dallas, 2011.

[7] Jürgen Habermas, *Legitimation Crisis*. London: Heinemann, 1971.

[8] J. Kallberg and B. Thuraisingham. "Cyber Operations: Bridging from Concept to Cyber Superiority," Joint Forces Quarterly, no.68.

[9] K. N. Waltz. "Nuclear myths and political realities," The American Political Science Review, Vol. 84, No. 3 (Sep., 1990), pp. 731-745 .