Strategic Analysis

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

Assessing India's Cyber Resilience: Institutional Stability Matters

Jan Kallberg

To cite this article: Jan Kallberg (2016) Assessing India's Cyber Resilience: Institutional Stability Matters, Strategic Analysis, 40:1, 1-5, DOI: 10.1080/09700161.2015.1116252

To link to this article: http://dx.doi.org/10.1080/09700161.2015.1116252

Published online: 07 Dec 2015.

Strategic Analysis, 2016
Vol. 40, No. 1, 1–5, http://dx.doi.org/10.1080/09700161.2015.1116252

Routledge
Taylor & Francis Group

Commentary

Assessing India's Cyber Resilience: Institutional Stability Matters

Jan Kallberg

The concept of strategic cyberwar

In this commentary, I will use strategic cyberwar theory[1] to explain why India has a higher level of cyber resilience than several of its potential adversaries. Even if India has challenges in its government-led cyber defence,[2] there are cyber resilience benefits to be drawn from the way Indian society operates, functions and is constitutionally designed and accepted by its constituents, independently of any cyber defence efforts. First, the concept of strategic cyberwar. A strategic cyberwar is a major conflict relying on heavy utilisation of digital means, a form of conflict that we have not yet seen but that is likely to be a potential threat a few decades into the future. Even if technological breakthroughs, adaptations and software development are accelerating at an increasingly high rate, the delay is not a technical issue. Technical evolutions in the software and services sphere are single lines of development. The complexity of cyber war increases with the time factor when cyber conflicts are likely thought at computational speeds. This require an acceptance of cyber as a form of war by itself because it operates in a battle space untangled from other forms of war fighting. Therefore, cyber cannot be seen as only an enabler in traditional defence.

Once cyber forces are created, these units need a doctrine, a strategy and the traditional capacity build-up of manpower, competence, equipment and unit ability that will take years. The lead times add up as it is necessary to add the political layer; politicians fund what they consider important and the funding process spans several years. New concepts take time to develop, with the main hurdle not technology but human immigration and the ability to put the new technology to proper systematic military use. A delay in military application of a novel concept is common. The first tanks appeared in 1916 and it took more than 30 years for them to be effectively used in battle. Helicopters were invented in the 1930s but it took until the 1960s before they found their role in the armed forces.

War is fought by humans, directed by military leaders and politicians, and the delay is the time needed for these actors to see the opportunity, organise the effort, find the technology providers, fund and procure what is needed for the future cyber forces.

Jan Kallberg is an Assistant Professor at the United States Military Academy (West Point) and a Research Fellow at the Army Cyber Institute at West Point.

In cyber matters, there is a tendency to overlook the human component. It is the people—either those attacking or those who are targeted—that decide the course of action. For a strategic cyberwar to be successful, it has to change human beliefs and the course of action.

A key question is how strategic cyber warfighting reaches a strategic outcome. A strategic outcome could be submission to the attacker's will or an escape from strategic submission. Cyber security tends to over-emphasise operational and tactical cyber engagements as strategic cyberwar, but there is no likelihood of a strategic outcome when the actions are not strategic.

This commentary argues that if a society does not risk being destabilised or severely degraded, there is no strategic outcome because small technical disruptions do not radically change a nation state's policies and politics. Theory is an overarching way of combining ideas, phenomena and facts, in a generalised form, to seek to explain specific outcomes. Theory's strongest tenet is predictability. Theory can serve as a guide to prepare for future events and ensure that their outcomes are favourable.

Strategic cyberwar theory

In lieu of existing theories, and as a starting point, I designed a theory that I named 'strategic cyberwar theory'. In strategic cyberwar theory, the attack strategy is to cyber attack the core of the institutional framework of an adversarial nation in pursuit of destabilisation. If a nation is destabilised, it can be subdued to foreign will and the ability for the current regime to execute their strategy evaporates due to loss of internal authority and ability. The theory's predictive power is strongest when applied to targeting theocracies, authoritarian regimes and dysfunctional experimental democracies, because the common tenet is weak institutions.[3]

In the region in which India has geopolitical interests, there are several other actors, Pakistan, the People's Republic of China and Iran, to mention a few. The actors that are likely to be adversarial are authoritarian, theocratic or totalitarian in constitutional design and lack different levels of democratic functionality and popular acceptance as legitimate regimes that serve the people's best interests.

Fully functional democracies, on the other hand, have a definite advantage in cyberwar; they have stable institutions that are accepted by their citizenry. Nations openly adversarial to democracies are in most cases totalitarian states that are close to entropy. The reason these totalitarian states are under their current regime is the suppression of the popular will. Any removal of the pillars of suppression, by destabilising the regime's design and the institutions that make it functional, will release the popular will. A destabilised and possibly imploding Iranian regime is a more tangible threat to the ruling theocratic elite than military information subsystems being hacked. Dictators fear the wrath of the masses.

Strategic cyberwar theory seeks to look beyond the actual digital interchange, the cyber tactics, and instead create the predictive power of how a decisive cyber conflict should be conducted in pursuit of national strategic goals. From an Indian perspective, strategic cyberwar theory supports Indian cyber resilience based on institutional stability.

The main discourse in cyber security is technical and tactical. The theme of how to conduct strategic cyberwar is not comprehensively addressed. Therefore strategic cyberwar theory is created utilising the political theories of Dwight Waldo that seek

to explain what holds regimes and government together, and turn these theories upside down to achieve entropy in targeted nation states.[4]

If states seek to conduct decisive cyberwar, it will not be achieved by anecdotal exploits, but instead by launching systematic destabilising attacks on the targeted society. In strategic cyberwar theory, the intellectual works of Dwight Waldo are utilised; Dwight Waldo's research studied what makes a great society and by doing so theoretized what holds a society together and the instutitutional stability that is needed to avoid chaos and entropy. Strategic cyberwar theory turns Waldo's theories upside down to create destabilisation of a society. The systematic approach seeks to use institutional weaknesses, popular sentiment and underlying opposition to the targeted government as force multipliers. Targeting can induce a sense of lack of control and failure to safeguard their citizenry. A nation, or any societal structure, is organised through institutional arrangement. These arrangements require a set of basic functionalities to operate within the institution to ensure its continued stability and functionality. Institutions make a state stable, a government sustainable and functional, even in a degraded environment. Each country is unique in its institutional arrangements and the societal importance of these arrangements.

A systematic institutional cyber attack can be visualised as the collapse of a building built with prefabricated elements, such as a parking garage, on a framework of concrete beams, pillars and decking. If pressure is distributed evenly over the construction, there is no risk of collapse. The building is safe. If instead the energy is concentrated on one or a set of the bearing elements of the building, it will collapse. Dwight Waldo's theoretical work explained what makes a nation state stable. Waldo focused his theoretical work and scholarly productions on factors that uphold and stabilise a society and was a leading political scientist and theorist for over 50 years. Waldo named five factors—legitimacy, authority, knowledge management, bureaucratic control, and confidence. Authority could be both external authority, by leading or in some cases suppressing a people, and internal authority within the bureaucracy and political structure.

Waldo's five factors summarise the pillars of any society and government. If a major automated attack can undermine these pillars, the targeted society is either weakened or at risk of implosion. Legitimacy means not only that the government is legally legitimised, but that it is capable and focused on the intention to deliver a 'good society' or in a dictatorship an 'acceptable society'. Legitimacy is a sliding scale and cannot be seen as a value that the society either does or does not have.[5] 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 utilise 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 the trust people have that the government will deliver the expected benefits and the removal of fear for the future. According to Waldo, feelings of vulnerability and fear of future events indicate the absence of confidence in government.

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

If a society is destabilised, the institutional stability—both national and local government together with societal cohesion—determines whether the country will slide into entropy or be resilient. A cyber conflict that affects the targeted government's legitimacy and authority will affect the trust and confidence the population has in the government's abilities. The distance to entropy is contingent on the trust and confidence the population has in their government. If the population distrusts the government and lacks confidence in the future delivery of unrestricted public goods in a fair and equal way, the distance to entropy is shorter than in a functional democracy with maintained trust and popular confidence.

Cyber resilience: functional public institutions matter

India's most likely potential adversaries are totalitarian states or experimental democracies, a term coined by political scientists for regimes that have democratic elements but still operate in a non-democratic framework. India benefits from its functional democracy and the ability to solve cleavages in a democratic manner, which over time increases the legitimacy of the government and the confidence that the government is pursuing the best interests of the people. During national challenges and national crises, the parliamentary system of India has been functional and there has been a continuum of functional democracy.[6]

Indian politics may have colourful moments and discussions, even corruption, but it is important to see that the basic system works. Elections lead to a change in government, courts are independent and may come to conclusions that challenge the existing political and economic powers, and an Indian voter who drops his ballot is more empowered than his Iranian counterpart. This Indian empowerment and acceptance of the way of government, how the society is ruled, generates a cyber resilience by default because the general population will not seek to overturn the government or stage massive riots in the event of a major cyber campaign that limits the government's influence and control. The Indian distance from daily life to societal entropy is longer than that of its potential authoritarian and totalitarian adversaries.

Even if Indian legitimacy, authority, control and popular confidence would be pressured under strategic cyberwar against India, it is likely that the level of cohesion, resilience and surviving trust is significantly higher than that of its potential adversaries under similar conditions. India already has in its constitutional design, societal framework and existing institutions a comparably higher level of cyber resilience—without a cyber defence force, a national implemented strategy or a fully trained cyber workforce. In cyber matters, the power of freedom and democracy is pivotal for cyber resilience.

Disclosure statement

No potential conflict of interest was reported by the author.

Notes

1. Jan Kallberg, Bhavani Thuraisingham and Erik Lakomaa, 'Societal Cyberwar Theory Applied: The Disruptive Power of State Actor Aggression for Public Sector Information Security', Paper

presented at the Institute of Electrical and Electronics Engineers (IEEE) European Intelligence and Security Informatics Conference (EISIC), Uppsala, 2013.
2. Nir Kshteri, 'India's Cybersecurity Landscape: The Roles of the Private Sector and Public–Private Partnership', *IEEE Security & Privacy*, May/June 2015, pp. 2–9.
3. Paul Brooker, *Non-Democratic Regimes: Theory, Government and Politics*, Palgrave MacMillan, New York, 1994.
4. Jan Kallberg, 2016. 'Strategic Cyberwar Theory – A Foundation for Designing Decisive Strategic Cyber Operations', *Cyber Defense Review*. Spring (Pre-Press). forthcoming.
5. Jürgen Habermas, *Legitimation Crisis*, Beacon Press, Boston, 1975.
6. Maya Tudor, *The Promise of Power: The Origins of Democracy in India and Autocracy in Pakistan*, Cambridge University Press, Cambridge, 2013.

ORCID

Jan Kallberg http://orcid.org/0000-0002-0609-6985