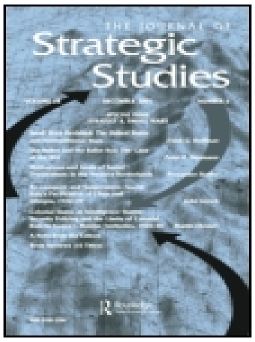

Journal of Strategic Studies

ISSN: 0140-2390 (Print) 1743-937X (Online) Journal homepage: https://www.tandfonline.com/loi/fjss20

How Probable is Cyber War? Bringing IR Theory Back In to the Cyber Conflict Debate

Timothy J. Junio

To cite this article: Timothy J. Junio (2013) How Probable is Cyber War? Bringing IR Theory Back In to the Cyber Conflict Debate, Journal of Strategic Studies, 36:1, 125-133, DOI: 10.1080/01402390.2012.739561

To link to this article: https://doi.org/10.1080/01402390.2012.739561

Published online: 06 Feb 2013.

The Journal of Strategic Studies, 2013
Vol. 36, No. 1, 125–133, http://dx.doi.org/10.1080/01402390.2012.739561

How Probable is Cyber War? Bringing IR Theory Back In to the Cyber Conflict Debate

TIMOTHY J. JUNIO

Center for International Security and Cooperation, Stanford University, California, USA and Department of Political Science, University of Pennsylvania, Philadelphia, USA

ABSTRACT Many well-established explanations for war suggest that cyber weapons have a greater chance of being used offensively than other kinds of military technologies. This response article introduces a research agenda for the study of cyber war, and offers an example – principal-agent problems in cyber operations – to demonstrate how rigorous theoretical and empirical work may proceed.

KEY WORDS: Cyber War, Information Technology, Computer Network Attack, Principal-agent, Command and Control

Two recent articles in the pages of this journal contribute to an important debate about how information technology (IT) influences international politics.[1] Thomas Rid and Adam Liff argue that cyber 'war' has never happened and probably will not happen. A fundamental problem with these articles is that Rid and Liff do not commit to a theoretical framework regarding the causes of war. Doing so yields an opposite conclusion: international relations theory identifies many mechanisms that may cause violent escalation with cyber weapons.

This brief response article explains why cyber war is sufficiently probable to merit serious attention from scholars and practitioners, and proposes a theoretical research agenda. First, domestic political factors – such as states' command and control over cyber operations – must be problematized. The principal-agent approach demonstrates

[1] Thomas Rid, 'Cyber War Will Not Take Place', *Journal of Strategic Studies* 35/1 (Feb. 2012), 5–32; Adam Liff, 'Cyberwar: A New "Absolute Weapon"? The Proliferation of Cyberwarfare Capabilities and Interstate War', *Journal of Strategic Studies* 35/3 (June 2012), 401–28.

how variation in incentives and preferences may make militaries more likely to favor cyber attack than other kinds of bureaucracies. This matters in societies with poor civilian control over the military. Second, the unique material qualities of IT must be evaluated alongside traditional mechanisms that cause war. For instance, the attribution problem and computational complexity in modeling cyber operations may increase the odds of inadvertent cyber war by causing states to retaliate against the wrong targets or miscalculate the potential costs and gains of attacking.

What is Cyber War? (Again…)

Rid and Liff do not define cyber war the same way, and there is no disciplinary consensus. Rid, Liff, and this author at least agree on the following: *cyber war is a coercive act involving computer network attack*. Network attack means information is disrupted, degraded, or destroyed. 'Coercive' means using force to change or preserve a political status quo. A point of contention is lethality, which Rid believes is necessary for cyber 'war'.[2] This is an extreme and undesirable requirement, particularly because (as Rid himself points out) non-lethal cyber attacks may be more costly than conventional warfare.[3] It is important to note that Rid focuses on network attack, whereas Liff considers a broader conflict process. This response addresses both.

The central point of Rid's article is that it is difficult to cause lethal effects with cyber weapons, and that politically motivated, instrumental cyber attack has never killed anyone.[4] While the empirics of his article are sound – he describes recent cyber attacks accurately – Rid never explains what causes war or makes war more or less likely. The arguments in his article are exclusively definitional, and do not directly support his title's assertion that 'Cyber War Will Not Take Place.'

Liff does better from a theoretical point of view; he links his article to the bargaining approach to war.[5] He does an excellent job of offering counterpoints to four arguments about why cyber attack may increase the probability of war. However, Liff never establishes why his reasonable views are more plausible than their alternatives. This is because he is not explicit about assumptions that are necessary for his arguments to hold, nor about the circumstances under which those assumptions break down. For example, Liff argues that private information may make war less likely because states poorly estimate

[2] Rid, 'Cyber War Will Not Take Place', 9.

[3] Ibid.

[4] Ibid., 6.

[5] Liff, 'Cyberwar: A New "Absolute Weapon"?, 422

the gains from cyber attack.[6] Although Liff is right to point out that ambiguity in cyber operations is important, he is wrong to assume the causal arrow points in one direction. Ambiguity can make war more *or* less likely, because it may lead states to overestimate their potential gains, overestimate their stealth, and/or underestimate their adversary's skill.

Finally, it must be recognized that *any* future war is a low probability event. Crafting claims that particular conflict scenarios are improbable is rather unimpressive; what is important to understand is the potential cost and probability of cyber war relative to other kinds of conflict.

Causes of Cyber War

The noted problems in the Rid and Liff articles could have been avoided by drawing on structured theoretical approaches that are common to the study of the causes of all kinds of warfare. What would such an approach look like? This response lacks the space to fully develop one, but recommends a way forward. Literally dozens of arguments have been advanced in the political science discipline regarding the causes of war, and very many of these offer reasons to believe cyber war is plausible or even probable.[7] An approach, advanced in James Fearon's modern classic 'Rationalist Explanations for War,' is to list assumptions that create an ideal condition in which war should never happen.[8] One way to structure scientific inquiry regarding the probability of cyber war is to examine how the unique material qualities of IT affect each of the assumptions. Table 1 offers a cursory version of such an analysis to identify priority areas for further study. Among a large number of revealed paths to cyber war, one – principal-agent problems involving the bureaucracies that conduct cyber operations – is detailed here to demonstrate the plausibility of specific mechanisms and what follow-on empirical work should look like.

Principal-Agent Problems

Rid and Liff appear to assume that states are unitary rational actors (URAs), and do not explain the domestic political processes whereby states make foreign policy choices. Empirically and theoretically, it is

[6] Ibid., 421.

[7] Jack S. Levy, 'The Causes of War and the Conditions of Peace', *Annual Review of Political Science* 1 (1998), 139–65.

[8] James D. Fearon, 'Rationalist Explanations for War', *International Organization* 49/3 (Summer 1995), 379–414.

Table 1. Bargaining Theory Assumptions and Cyber War

	Assumption	IT Makes This Assumption…	Justification
1	States are unitary rational actors (URAs) in their decision-making	Less tenable	Military organizations often favor offensive cyber operations, whereas other kinds of bureaucracies prefer a defensive orientation. Political command and control over these organizations varies between states.
2	War is costly	Less tenable	Cyber operations have the potential to dramatically change cost calculations, as they have relatively low material and labor costs, and lower retaliation and audience costs when states conceal attribution.
3	People do not go to war for pleasure	Less tenable	Demonstrating skill through penetrating adversary networks is central to the hacker ethos and is a value in itself; combined with poor command and control, could lead cyber bureaucrats to inadvertently create or escalate political disputes.
4	States know that, in principle, there is some true probability that one side will win (even if they disagree in their estimates)	Same as other kinds of warfare	–
5	Leaders are risk-averse or risk-neutral	Same as other kinds of warfare	–
6	Issues are divisible (e.g., there is a continuous range of possible settlements, made possible by	Same as other kinds of warfare	–

(*continued*)

Table 1. (*Continued*)

	Assumption	IT Makes This Assumption…	Justification
	mechanisms like side-payments and issue-linkage)		
7	States have an equivalent ability to make assessments about outcomes	Less tenable	Modeling network operations is highly complex and computationally demanding; routing and software change frequently. States are highly likely to reach divergent assessments, which may narrow the bargaining range.
8	States have perfect information about their capabilities and intentions and those of their adversaries	Less tenable	States have very great difficulty achieving confident, timely cyber attribution.
9	Actions are purposeful ('accidents' do not happen when it comes to foreign policy)	Less tenable	Cyber operations for espionage and maintaining network access occur regularly, and constitute most of the sequence required for an offensive act that results in violence. With a large number of states constantly seeking to penetrate each other's networks, it is a probabilistic certainty that accidental network disruptions will happen.

important to relax the URA assumption and problematize who has formal and actual release authority over cyber weapons. The principal-agent approach, for instance, works from the premise that individuals and organizations often vary in their incentives and preferences, which could make war beneficial for some at the cost of others.[9] This and related thinking inform how scholars study other military technologies, such as nuclear weapons. Scott Sagan points out that although

[9] David M. Kreps, *A Course in Microeconomic Theory* (Princeton UP 1990).

unauthorized nuclear war is improbable, it is sufficiently probable that people should worry a great deal about command and control (C2) issues.[10] Many anecdotes echo Sagan's work. For example, a Russian general was asked during the Cold War about his backup plan in the event he could not open the safe containing his nuclear launch codes. His answer was that he would bash the safe open with a sledgehammer he kept nearby![11]

Consideration of how bureaucracies do what they do – like keeping emergency nuclear war sledgehammers – is of critical importance to the cyber C2 question. Although controlling large organizations is a core function of militaries, the conduct of cyber operations is different from other kinds of activity in a way that greatly magnifies the 'strategic corporal' problem. This is because constant cyber operations other than war decrease the bureaucratic friction that normally alerts superiors to aberrant behavior. In the case of nuclear weapons, a long chain of events is required before unauthorized activities occur. Someone probably would notice a crazed general using his sledgehammer on the launch codes safe, turning keys, fueling missiles, and so on. In contrast, it is a core function of cyber bureaucrats to access adversary networks *constantly*, and to develop push-button solutions to minimize lags during war. Furthermore, if the perception that cyber weapons are non-lethal comes to be widely perceived (as Rid would prefer), it is reasonable to conclude that the threshold for their use will be lower than other kinds of weapons – even if the cost of cyber attacks is greater.

While weak C2 is a *necessary* condition for a war caused by principal-agent problems, it is not *sufficient*, because bureaucracies (agents) must also have different incentives or preferences from their populations or leaders (the 'principals'). A deep political science literature argues that militaries are more prone to favor offensive operations than other kinds of bureaucracies.[12] Early evidence suggests that this 'cult of the offensive' operates regarding cyber warfare. James Cartwright, the former Vice Chairman of the US Joint Chiefs of Staff, calls for the United States to engage in more offensive cyber operations, and reportedly created a bureaucracy to that end.[13] This perspective

[10] Scott Sagan, *The Limits of Safety* (Princeton UP 1995).

[11] Vadim Koval, 'Russian Missile Forces Have "Safe Busting" Sledgehammer', *Rianovosti*, 2012.

[12] Stephen Van Evera, 'The Cult of the Offensive and the Origins of the First World War', *International Security* 9/1 (1984), 58–107.

[13] Andrea Shalal-Esa, 'Ex-US general urges frank talk on cyber weapons', *Reuters*, 6 Nov. 2011; David E. Sanger, *Confront and Conceal* (New York: Crown 2012), 191–3.

exists in other countries; officials with South Korea's Cyber Command believe that 'the best defense is a good offense', and that they should preemptively disable menacing foreign servers.[14] Chinese military textbooks recommend 'information offensive through computer network attack' in advance of conventional warfare.[15] In contrast, nearly all other bureaucracies – such as those responsible for diplomacy, law enforcement, and homeland security – appear oriented toward cyber defense.

If this offensive mindset is observed in countries where civilians have firm control over military organizations, then what is the risk from countries with different civil-military relations?[16] The thought of weak or military-dominated states possessing advanced cyber capabilities is troubling, to say the least, and offers highly plausible paths to cyber war. An example, North Korea, already has demonstrated offensive tendencies, as that government appears to have conducted disruptive and destructive cyber attacks.[17]

Many potential paths to war result from a combination of 'cult of the offensive' reasoning and weak C2. One is for militaries to justify cyber attack as acts of self-defense or preemption. Another is for militaries to conduct offensive cyber operations without informing their superiors. Yet another is the potential for offensive biases to make them more easily fall bait to 'false flag' operations. These are merely derivatives of principal-agent problems that arise among politically motivated actors; the outlook worsens when considering other incentives, such as profit, that may lead corrupt bureaucrats to sell lethal skills or software to the highest bidder.

Conclusion

So, how much should scholars and practitioners care about cyber war? A belief that cyber war is hyped appears to have motivated Rid and Liff to pen their pieces. A satisfying answer must explain at least two things: the destructive potential of cyber war, and the probability that it will happen. It appears uncontroversial that, if cyber war happens, it will be

[14] Interview, South Korean Cyber Command officers, Seoul, January 2012.

[15] Yuliang Yuliang Zhang, *The Study of Campaigns [Zhanyi xue]* (Beijing: National Defense UP 2006), quoted in Roger Cliff *et al.*, *Shaking the Heavens and Splitting the Earth* (Santa Monica, CA: RAND 2011), 98.

[16] For an introduction to variation in civil-military relations, see Peter Feaver, *Armed Servants* (Cambridge, MA: Harvard UP 2003).

[17] 'N. Korean Ministry behind July cyber attacks: spy chief', *Yonhap News Agency*, 30 Oct. 2009; Kim Sue-Young, 'Spy chief says cyber attacks work of N Korea', *Korea Times*, 30 Oct. 2009.

highly costly even if not lethal. Few contest the idea that a successful and sustained degradation of military capabilities, deprivation of civilian services, destruction of financial records, or other such ‘digital Pearl Harbor’ scenarios, would be pretty bad.

On the other hand, there is little agreement in academic or policy circles regarding whether or not cyber war will happen. This response offers an important corrective to narratives that cyber war is improbable. A small number of premises lead to a conclusion that cyber war is, at a minimum, plausible enough to merit serious attention. Further research would do well to commit to theoretical paradigms, such as the approach recommended in Table 1. This kind of rigorous scholarship is a prerequisite to reducing the incidence of cyber conflict and avoiding cyber war.

Acknowledgements

The author thanks Alex Weisiger, Jake Shapiro, Tom Mahnken, Joe Lin, and John Stevenson for their thoughts on earlier drafts.

Note on Contributor

Timothy J. Junio (**Tim**) is a doctoral candidate of political science at the University of Pennsylvania and a predoctoral fellow at the Center for International Security and Cooperation (CISAC) at Stanford University. He also develops new cyber capabilities at the Defense Advanced Research Projects Agency (DARPA).

Bibliography

Cliff, Roger *et al.*, *Shaking the Heavens and Splitting the Earth* (Santa Monica, CA: RAND 2011).

Evera, Stephen Van, ‘The Cult of the Offensive and the Origins of the First World War’, *International Security* 9/1 (1984), 58–107.

Fearon, James D., ‘Rationalist Explanations for War’, *International Organization* 49/3 (Summer 1995), 379–414.

Feaver, Peter, *Armed Servants* (Cambridge, MA: Harvard UP 2003).

Koval, Vadim, ‘Russian Missile Forces Have “Safe Busting” Sledgehammer’, *Rianovosti*, 2012.

Kreps, David M., *A Course in Microeconomic Theory* (Princeton UP 1990).

Levy, Jack S., ‘The Causes of War and the Conditions of Peace’, *Annual Review of Political Science* 1 (1998), 139–65.

Liff, Adam, ‘Cyberwar: A New “Absolute Weapon”? The Proliferation of Cyberwarfare Capabilities and Interstate War’, *Journal of Strategic Studies* 35/3 (June 2012), 401–28.

‘N. Korean Ministry behind July cyber attacks: spy chief’, *Yonhap News Agency*, 30 Oct. 2009.

Rid, Thomas, ‘Cyber War Will Not Take Place’, *Journal of Strategic Studies* 35/1 (Feb. 2012), 5–32.

Sagan, Scott, *The Limits of Safety* (Princeton UP 1995).
Sanger, David E., *Confront and Conceal* (New York: Crown 2012).
Shalal-Esa, Andrea, 'Ex-US general urges frank talk on cyber weapons', *Reuters*, 6 Nov. 2011.
Sue-Young, Kim, 'Spy chief says cyber attacks work of N Korea', *Korea Times*, 30 Oct. 2009.
Zhang, Yuliang, *The Study of Campaigns [Zhanyi Xue]* (Beijing: National Defense UP 2006).