Reliance on Third Parties: Understanding the Problem on Land and in Cyberspace

Jon Lindsay
University of California Institute on Global Conflict and Cooperation (IGCC)

There are two very different conversations about the nature and future of warfare in defense intellectual circles. The first centers on irregular threats such as insurgents, terrorists, and armed gangs and the suitability of doctrine such as counterinsurgency (COIN) and counterterrorism (CT) to deal with them. The second worries about novel threats in cyberspace created by societal dependence on computer networks and the international proliferation of hacking tools. These topics appear to be radically distinct: the former ponders a gritty "war among the people" in the developing world while the latter fears high-tech confrontation in cyberspace between advanced industrial powers. The differences are real enough, to be sure, but there may also be some important similarities. Understanding these similarities—and in particular the varieties of information imperfections generated by indirect action through third parties—is important for guiding intelligence collection, analysis, and protection priorities in both irregular warfare (IW) and cyber operations (CO).

The history of irregular warfare goes back centuries, but the tragedies of 9/11, Iraq, and Afghanistan newly energized discussion of COIN and CT and provided examples aplenty. In the past decade the intellectual pendulum has swung from frustration at the inability of conventional military force to combat irregular threats, to near euphoria at the rediscovery of COIN doctrine from an earlier era and its apparent triumph in Iraq, and back again to disillusionment at the failure of COIN to fix the mess in Afghanistan. Even the efficacy of COIN in Iraq now appears dubious in recognition of other forces acting simultaneously, such as the Sunni realignment or "Awakening" in Anbar and the culmination of ethnic cleansing in Baghdad.[i] Critical scholars have argued, including colleagues on another panel in this

conference, that COIN manuals which focus on protecting the population and developing nation-state infrastructure neglect the violent and highly localized bargaining processes which characterize civil war and state building.[ii] Military personnel in this environment must rely on third parties—indigenous security forces, armed militias, local contractors, tribal elites—in order to make any progress, but their loyalty, competence, or efficacy cannot be taken for granted. Even CT, carried out more unilaterally by special operations forces or armed drones, must contend with this restive milieu as it reacts adversely to errors and successes alike. Moreover, the military and civilian agencies tasked with monitoring and enforcing the behavior of all these third parties face formidable internal coordination problems.

By contrast the history of information security and electronic warfare goes back only decades, but even that is oft forgotten in the very recent eruption of excitement over cybersecurity.[iii] These ideas invert the 1990s notion of a "revolution in military affairs" (RMA): whereas computer networks once enabled radical offensive military advantagess, they now create radical defensive vulnerability (or equivalently, radical offensive advantage for the hacker). Many now fear that ubiquitous military and economic dependence on cyberspace enables hackers to launch a "digital Pearl Harbor" or "cyber 9/11" or to siphon away intellectual property leading to "death by a thousand cuts."[iv] The most ominous rhetoric conjures up images of a "new nuclear age" with visions of massive societal paralysis. As Michael McConnell, former U.S. Director of National Intelligence, states, "cyber-war mirrors the nuclear challenge in terms of the potential economic and psychological effects."[v] Yet the only historical example of cyber attack on physical infrastructure, the Stuxnet infection of Iranian centrifuge controls, produced only minor and temporary disruption while the vast majority of "attacks" have merely been online espionage, crime, and "hacktivist" protest.[vi] At the same time the sheer scale of cyber espionage, primarily from China against expatriate political targets and Western economic interests, is alarming.[vii] However, cybercrime damage estimates are notoriously overinflated and cyber-espionage estimates are likely as well if one considers the formidable difficulties of analyzing and acting on petabytes worth of stolen data.[viii] Indeed, present excitement over cyber warfare may be headed for empirical disillusionment not unlike that which met previous enthusiasm for COIN doctrine.[ix]

While the problems of CO and IW appear to fall at the extreme ends of the spectrum of technological and cultural perspectives on war, there may be some value in thinking about them together. The analogical bridge is the recognition that both types of operation require extensive reliance on third parties. IW works "by, with, and through" indigenous militias and local security forces amid a complex milieu of social interactions. CO works through infrastructure invented, owned, and administered by civilian entities and teaming with highly varied private transactions. The framing of CO as a type of IW helps to direct attention toward the social and political foundations of conflict, something largely missing from the narrowly technological discourse of cyberwar.

Following a decade of ambiguous operational and strategic experience in Iraq and Afghanistan, together with broader comparative study of other civil wars in history, there is growing appreciation that IW is a messy, uncertain, and expensive business, shot through with information imperfections and intelligence failures. There is far less appreciation for the ways in which complex bargaining also constrains and enables CO. All action in cyberspace, from this perspective, is indirect action. It is indirect not only through remote machines and precompiled code, but also through users, developers, administrators, and managers everywhere and constantly engaged in maintaining, configuring, and adapting systems. The loyalty, competence, and results of all these remote resources cannot be taken for granted, and the coordination of domestic and international stakeholders involved in cybersecurity makes the vaunted COIN interagency problem look easy by contrast. By examining CO in terms of IW, with a focus on the problems of understanding and controlling third-party agents, we might better understand the sociotechincal uncertainties which limit the predictability and efficacy of cyber operations.

Furthermore, if the ostensibly technical domain of CO depends on political interactions, then ironically enough, militaries often shoehorn the ostensibly political domain of IW into a computational framework. Military bureaucracies tend to approach warfare algorithmically, looking for procedures and templates to apply to a doctrinally defined set of inputs in order to produce victory. Yet while procedural heuristics can help to guide staff and operational behavior, they tend to elide the essential agency of enemies, allies, and bystanders who don't

follow the rules. The third party problem, whether in IW or CO, is a problem of indirect action imperfectly controllable in its context, whereas the doctrinal fragility of both is a problem of direct algorithmic action imperfectly suited to its context. Computer networks are more complexly social than we usually appreciate, and social organizations can be rigidly computational.

How does this all tie into the panel's theme of intelligence and security assistance? Security assistance in DOD parlance encompasses any assistance to foreign militaries, whether in training, equipment, or intelligence, but we can broaden this somewhat to include irregular allies as well as more formal state entities. As an active duty intelligence officer I have worked with SEALs in Latin America and Iraq who had an unofficial motto for FID, or Foreign Internal Defense. FID is a type of security assistance known which involves training and equipping foreign security services. They described FID as "Training tomorrow's enemy today." Cynical, yes, but it goes right to the heart of the problem of dealing with proxies. Their loyalty is not assured. Neither is their competence nor their results. There is a lot of uncertainty associated with reliance on proxies, and this uncertainty poses an intelligence problem: substantively as a collection requirement to reduce uncertainty, and materially as a threat to the operational security of shared intelligence. These major problems associated with proxies in either IW or CO are informational, and by extension, intelligence problems. Without a more refined understanding of the indirect nature of such conflict and the ways in which this indirection can break down or lead to unintended consequences, intelligence collection, analysis, and protection efforts will lack direction.

---

[i] See commentary by Jon Lindsay and Austin Long in *International Security* (Spring 2013) on Stephen Biddle, Jeffrey A. Friedman, and Jacob N. Shapiro, "Testing the Surge: Why did Violence Decline in Iraq in 2007?" *International Security* (2012): 1-13

[ii] Jackson, Rovner, Staniland, Hazelton

[iii] Michael Warner, "Cybersecurity: A Pre-History," *Intelligence and National Security* vol. 27, no. 5 (2012): 781-799

[iv] Obama 2013 SOTU: "America must also face the rapidly growing threat from cyber-attacks. We know hackers steal people's identities and infiltrate private e-mail. We know foreign countries and companies swipe our corporate secrets. Now our enemies are also seeking the ability to sabotage our power grid, our financial institutions, and our air traffic control systems. We cannot look back years from now and wonder why we did nothing in the face of real threats

to our security and our economy." http://www.whitehouse.gov/the-press-office/2013/02/12/president-barack-obamas-state-union-address

[v] Mike McConnell, "Mike McConnell on How to Win the Cyber-War We're Losing," *Washington Post* (28 February 2010). This is not a uniquely American perspective. PLA strategists Ye Zheng and Zhao Baoxian argue that "just as nuclear war was the strategic warfare of the industrial age, network warfare will be the strategic warfare of the information age." In "How Do You Fight a Network War?", *Zhongguo Qingnian Bao Online*, 3 June 2011.

[vi] Jon Lindsay, "Stuxnet and the Limited Future of Cyber Warfare" (2013); Thomas Rid, "Cyber War Will Not Take Place," *Journal of Strategic Studies* vol. 35, no. 1 (2011): 5-32

[vii] Office of the National Counterintelligence Executive, *Foreign Spies Stealing US Economic Secrets in Cyberspace*, Report to Congress on Foreign Economic Collection and Industrial Espionage 2009-2011, October 2011; Information Warfare Monitor, *Tracking Ghostnet: Investigating a Cyber Espionage Network*, Secdev Group and University of Toronto Citizen Lab, 29 March 2009, http://www.scribd.com/doc/13731776/Tracking-GhostNet-Investigating-a-Cyber-Espionage-Network

[viii] Ross Anderson, Chris Barton, Rainer Bohm, Richard Clayton, Michel J.G. Van Eeten, Michael Levi, Tyler Moore and Stefan Savage, "Measuring the Cost of Cybercrime," Workshop on the Economics of Information Security (June 2012)

[ix] Excitement over the technical possibilities of cyberspace provides a welcome relief from the messy indecisiveness of COIN, but reality is sure to intrude messily again in future conflicts. The ascendency of COIN ideas in the 2000s, preceded by RMA in the 1990s and followed by cyber warfare in the 2010s, suggests a longer term pendulum in defense intellectual fashions between technology- and society-centric visions of war. From the techno-centric problem of nuclear confrontation and large scale conventional conflict, to the reorientation toward guerilla warfare in Vietnam, to the rise of the RMA in response to the European central front and later internet millennialism, to the "population centric" adventures in Iraq and Afghanistan, on to the contemporary fretting over cyberspace vulnerabilities, these polar extremes are regularly rediscovered every decade or so. Despite the oscillating rhetorical emphasis, the dichotomy between technology and society centric warfare is a false one; Lindsay 2013.