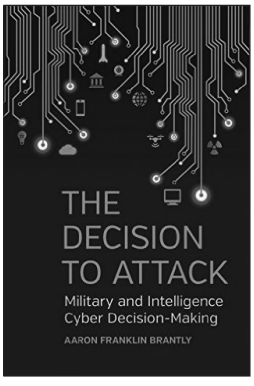
Book Review



The Decision to Attack: Military and Intelligence Cyber Decision-Making

Aaron Franklin Brantly

University of Georgia Press, 2016, 226 pp.

Reviewed by Dr. John G. Breen
Distinguished Chair for National Intelligence Studies, U.S. Army Command and General Staff College, and CIA Representative to the U.S. Army Combined Arms Center

"The Russian government hacked into the e-mail accounts of top Democratic Party officials in order to influence the outcome of the 2016 U.S. Presidential election." This is a clear statement of guilt, definitive and direct, with little room for doubt. An attack like this demands a response. Doesn't the manipulation of an American election warrant some sort of retaliation? Could this be an act of war? So why isn't the U.S. (at least overtly) doing more in response?

Well, read closely the official statement about the Russian hacking from the Department of Homeland Security and the Director of National Intelligence.[1] In colloquial intelligence-speak, it doesn't really say the Russian government is definitively responsible for the compromise. The statement notes merely "confidence" that the Russian government "directed" the compromise and offers as evidence only that these attacks were "*consistent with* the methods and motivations of Russian-directed efforts." The careful use of indefinite phrases such as "consistent with", "we believe" or "we judge" leaves inconvenient room for reasonable doubt and plausible deniability about who actually conducted the attacks and who is ultimately accountable.

These types of assessments, as dissembling assurances go, sound eerily familiar, ala the 2002 Iraq WMD National Intelligence Estimate. Was there WMD in Iraq or not? Before the invasion, the community certainly said "we judge" that there was. Think of it this way; no mafia don could be convicted in a court of law by a prosecutor asserting only that the state was "confident" the individual was guilty. Offering as proof that the murder was "consistent with the methods and motivations of Mafia-directed efforts" is not sufficient. Did the don order the hit, conduct the act himself, or is he being blamed as a convenient scapegoat? These intelligence assessments simply do not seem to provide the unambiguous attribution necessary to reasonably contemplate retaliation.

This lingering ambiguity is a key issue addressed in Aaron Brantly's 2016, *The Decision to Attack: Military and Intelligence Cyber Decision-Making*. An Assistant Professor at the U.S. Military Academy, Brantly provides a detailed academic exploration of cyber warfare, seeking to better understand how states interact within cyberspace. He posits that states should generally be considered rational actors and therefore will rank order their likely actions in cyberspace based on positive expected utility, i.e. how successful these actions will be compared to the risks they

engender (expected utility theory). *Decision to Attack* is an excellent treatment of this crucial domain, packed densely with insight into a deceptively pithy 167 pages.

The research encapsulated in *Decision to Attack* suggests the key determinant in a state choosing to undertake an offensive cyber-attack is anonymity. That is to say, a state's ability to keep its attack secret as it is being undertaken, as well as its capacity to hide or at least obscure the origin of the attack afterward. There is no barrier to action if there is no risk of retribution. As Brantly notes, the hurdle for choosing offensive cyber-attacks is extremely low when a state can assume some level of anonymity:

"Anonymity opens Pandora's box for cyber conflict on the state level. Without constraints imposed by potential losses, anonymity makes rational actors of almost all states in cyberspace. Anonymity makes it possible for states at a traditional power disadvantage to engage in hostile acts against more powerful states…. Because anonymity reduces the ability to deter by means of power or skill in most instances, the proverbial dogs of war are unleashed. If the only constraints on offensive actions are moral and ethical, why not engage in bad behavior? Bad behavior in cyberspace is rational because there are few consequences for actions conducted in the domain."[2]

Brantly does offer some hope that states will not rationally engage in "massively damaging" cyber-attacks, given that with greater complexity and scale these attacks become less likely to be kept truly unattributable. His assertion seems to be that these states, particularly those smaller states with less traditional or conventional power (military and otherwise), will focus on small to mid-range types of attacks. That said, even seemingly minor attacks can apparently lead to unintended significant impacts, certainly if these pile up over time -- a cyber domino effect. For example, a relatively small-scale compromise of an individual's email account, followed by propagation of resultant inflammatory "revelations" seeded into the press and on-line social media, might lead to the upending of an otherwise democratic election.

Given the demonstrated importance of secrecy and obfuscation in the cyber domain, Brantly appears to argue in *Decision to Attack* that cyber-attacks should be considered a type of covert action. He points out that the U.S. government's approach to cyberspace has to this point relied on the military, with Admiral Mike Rogers currently the commander of both the National Security Agency and Cyber Command (CYBERCOM). To Brantly, this indicates the president has given the military, and not the Central Intelligence Agency (CIA), the lead as the main covert operator in the cyber domain. He offers in criticism that this arrangement may run counter to Executive Order 12333, which provides lanes in the ethical/moral superhighway for the intelligence community. Brantly indicates though that the Department of Defense's capacity to address the scale of the problems identified in cyber make this designation "appropriate."[3]

While perhaps not the major focus of Brantly's research, the implications of relying on the military to conduct these types of offensive operations are perhaps worth further exploration. There are reasons the CIA was designated and utilized during the cold war to be the primary organization responsible for covert action. In sum, it seems to have everything to do with plausible deniability. If you are caught by an opposing state in the conduct of covert action while in uniform, this might be considered an act of war. Is it any less so in cyber? Perhaps.

In March 2015 the CIA embarked on an unprecedented "modernization" effort designed to "ensure that CIA is fully optimized to meet current and future challenges," largely by pooling analytical, operational and technical expertise into ten new Mission Centers.[4] A new operational component -- the Directorate of Digital Innovation (DDI) -- was also added to the existing four

Directorates: Operations, Analysis, Science and Technology, and Support. The DDI is said to be focused on "cutting-edge digital and cyber tradecraft and IT infrastructure."[5] Public statements from the Agency have highlighted the importance of culture, tradecraft, and knowledge management in this new Directorate, stressing the DDI's role in support of the CIA's clandestine and open source intelligence collection missions.[6,7]

In a July 2016 speech to the Brookings Institution, CIA Director John Brennan discussed the mission of the newly created DDI and the risks posed by cyber exploitation. For example, Brennan suggested the Arab Spring revolts were influenced by on-line social media's ability to swiftly facilitate social interaction and cause destabilization, that cyber could be used to sabotage vital infrastructure, or might be used by terrorist organizations to indoctrinate potential lone wolf actors.[8]

CIA of course looks to exploit this same cyber domain to its own ends. In CIA's vernacular, destabilization then is "covert cyber-based political influence"; sabotage is a "cyber-facilitated counter proliferation covert action"; and indoctrination becomes an "on-line virtual recruitment." What distinguishes between these actions –- anarchic destabilization versus covert cyber-based political influence -- is the intent, noble or ignoble, of the perpetrator.

Cyber espionage then at least might be thought to follow many of the same tradecraft norms and to be constrained by many of the same rules and self-imposed restrictions as real-world, "Great Game" espionage and especially some types of non-lethal covert action. For example, if caught in the midst of a recruitment operation against a foreign diplomat in some capital city, that country's government typically would simply kick the offending CIA officer out of the country, declaring the individual *persona non grata*. One could say there are systems in place, most informal, that allow for a bit of espionage to be conducted without causing conflagration. This is especially true when dealing with near-peer competitors, as evidenced by decades of cold war intrigue. CIA was chosen, for example, to conduct covert action in Afghanistan during the cold war in order to avoid an act of war incident. CIA's actions against the Soviet occupation were no less deadly, but use of foreign cutouts and misattributable materiel, i.e. tradecraft, allowed for plausible deniability and lack of attribution. The Soviets could "judge" all they wanted that the U.S. was behind their mounting losses, but without proof, this was meaningless.

CYBERCOM, the closest military counterpart to the DDI, was created as a joint headquarters in 2009. Unlike the CIA's DDI clandestine collection posture, CYBERCOM's stated mission appears much more broadly focused on traditional (though still cyber) offensive operations and network defense, i.e. "ensure U.S./Allied freedom of action in cyberspace and deny the same to our adversaries."[9] U.S. military joint doctrine on cyberspace operations is filled with otherwise conventional military terms such as "fires" and "battle damage." A cyber weapon deployed against an adversary on the cyber battlefield can be called a "payload."

The military's cyber effort also appears to be somewhat encumbered by familiar bureaucratic challenges, not the least of which involves nominal joint efforts to operate in a domain not easily divvied up amongst services used to "owning" a particular geographic space, i.e. ocean, air, land. As noted by an Army strategist working on the Joint Staff Directorate for Joint Force Development:

"The opportunity for one service to infringe on, or inadvertently sabotage, another's cyberspace operation is much greater than in the separate physical domains. The command-and-control burden and the risk of cyberspace fratricide increase with the number of cyberwarriors from four different services operating independently in the domain."[10]

How much greater then is the challenge in deconflicting operations between these disparate DoD cyber operators and those in the intelligence community and CIA's DDI, all engaged on the same cyber field of play? If CIA has worked for years to gain cyber access to a particular source of protected information, and another actor wants to "deliver a payload" against that target, who decides which mission is most important? Do we choose the intelligence collection activity we need to better understand the enemy or is it the cyber-attack that cripples an adversary's critical capability? And is there an advantage in having the military or a civilian organization conduct either of these covert action operations? These and many other important questions that spin off from reading *Decision to Attack* await further exploration.

Ultimately this decision-making should perhaps extend beyond the inside view taken by the operators from CYBERCOM or the CIA's DDI. The process will hopefully include policy-makers struggling with how and why to use cyber as either an offensive tool or a tool of espionage. Brantly provides the reader with these delineations, offering definitions of, for example, cyberattack versus cyber exploitation. He also provides a solid starting point for a discussion about which of these approaches is most appropriate and a framework in which to understand our own and our adversary's potential decision-making processes. There's more to be said and in this evolving domain there is much more to understand, but *Decision to Attack* should be in the library of those hoping to make the right call when it comes time to act. ***IAJ***

Notes

1 https://www.dni.gov/index.php/newsroom/press-releases/215-press-releases-2016/1423-joint-dhs-odni-election-security-statement

2 Brantly, Aaron Franklin. *The Decision to Attack: Military and Intelligence Cyber Decision-Making,* University of Georgia Press, 2016, pgs. 158-159.

3 Ibid, pgs. 123-124.

4 https://www.cia.gov/news-information/press-releases-statements/2015-press-releases-statements/cia-achieves-key-milestone-in-agency-wide-modernization-initiative.html

5 https://www.cia.gov/news-information/speeches-testimony/2016-speeches-testimony/director-brennan-speaks-at-the-brookings-institution.html

6 Ibid, https://www.cia.gov/news-information/press-releases-statements/2015-press-releases-statements/cia-achieves-key-milestone-in-agency-wide-modernization-initiative.html

7 https://www.cia.gov/offices-of-cia/digital-innovation

8 Ibid, https://www.cia.gov/news-information/speeches-testimony/2016-speeches-testimony/director-brennan-speaks-at-the-brookings-institution.html

9 https://www.stratcom.mil/factsheets/2/Cyber_Command/

10 Graham, Matt. U.S. Cyber Force: One War Away, *Military Review,* May-June 2016, Vol 96, No. 3, Pg. 114.