AIR & SPACE POWER JOURNAL - VIEW

Air, Space, and Cyberspace: Reinvigorating Defense of US Critical Infrastructure

Maj Lou Nguyen, USAF
Lt Col Jeremy L. Sparks, USAF

Disclaimer: The views and opinions expressed or implied in the Journal are those of the authors and should not be construed as carrying the official sanction of the Department of Defense, Air Force, Air Education and Training Command, Air University, or other agencies or departments of the US government. This article may be reproduced in whole or in part without permission. If it is reproduced, the Air and Space Power Journal requests a courtesy line.

> *"We have proven that by doing evil deeds, retribution does not come."*
>
> —Unidentified GandCrab ransomware proprietor

In June 2019, the purported masterminds behind the ransomware known as GandCrab announced their retirement from running a global computer malware distribution operation.[1] In the relatively short span of 15 months, GandCrab managed to rake in a record-breaking $2 billion in ransom payments.[2] The commercialization of cybercrime services by the likes of GandCrab, akin to the types of Infrastructure-as-a-Service and Software-as-a-Service commodities offered by more legitimate commercial cloud vendors, demonstrate that cybercriminal organizations are increasing in sophistication and ability. GandCrab's ransomware scheme's size and scope, and the temerity and impunity in which they operated, indicate the daring yet mercurial nature of modern malicious cyber actors, particularly advanced persistent threat (APT) groups.[3] If governments and law enforcement agencies were unable to stop, much less identify and prosecute, an overtly criminal entity like the gang behind GandCrab, what hope is there to prevent more serious threat actors from targeting critical infrastructure networks and systems? Malicious cyber actors continue to operate with such audacity for two primary reasons. First, the internet offers malicious cyber actors a level of anonymity that is difficult to counter without sufficient resources and determination.[4] Second, even if the identities of threat actors behind the malicious cyber activity are established, they typically encounter limited or no consequences, such as financial penalties, criminal prosecution, a military response, and so on.[5] We argue that through a combination of policy changes, organizational improvements, revamping of existing models, and increased threat actor identification efforts, air, space, and cyber forces can help meet and mitigate the threat malicious cyber actors pose to the national security of America.[6]

Fortunately, the US is already well on its way in addressing the various policy gaps that allow APTs to thrive. First and foremost, the *2011 Department of Defense (DOD) Strategy for Operating in Cyberspace* set the tone for organizing cyber forces, charging US Cyber Command (USCYBERCOM) with responsibilities hitherto, and establishing partnerships for collective cyber operations. Additionally, the 2011 DOD cyber strategy explicitly states that the DOD reserves the right to respond to cyber threats appropriately.[7] The most recent iteration of this strategy, the *2018 Department of Defense Cyber Strategy*, articulates a more mature and vigorous approach. The DOD, principally through USCYBERCOM, will persistently confront malicious cyber activity and defend US critical infrastructure.[8]

To that end, senior US officials have recently credited USCYBERCOM with conducting operations against Russian state-sponsored hackers. For example, USCYBERCOM is reported to have disrupted Russian information operation campaigns aimed at interfering with the 2016 US midterm elections.[9] While the Pentagon deemed the operations a success, some cybersecurity experts weren't as convinced that they successfully countered foreign interference. These operations, and the skeptical responses from cybersecurity pundits, highlight a paradox in how the US is addressing APTs.[10] Since 2011, the US has reserved the right to use military force in retaliation against cyber attacks. Still, despite repeatedly stating that it is willing to engage adversaries targeting the homeland in the cyber domain kinetically, the US has, in very few instances, acted against said adversaries in meaningful ways.[11] This disconnect between what the US states as strategy and the actions the government is willing to take to back up those assertions, is well understood by APT actors. One country taking a different approach to protecting its sovereignty in cyberspace is Israel.

In May 2019, the Israeli Defense Forces (IDF), amid an escalating conflict with Hamas, launched an airstrike targeting a Hamas cyber unit that was attributed to conducting cyber operations against Israel.[12] The IDF reported that its cyber forces identified the geographical location of a Hamas cyber unit and coordinated with the Israeli Air Force for kinetic actions. Soon after the coordination, Israeli air assets employed precision munitions against the Hamas cyber actors and equipment, destroying the specific rooms of the building where Hamas was conducting its cyber operations.[13] The ability to attribute, geolocate, and quickly target menacing cyber actors via kinetic means, represents an evolution of multi-domain operations. The US can develop and employ similar synchronization of air, space, and cyberspace to ensure that "evil deeds" do not go unpunished. Being able to impose costs, mainly through kinetic means, will be a keystone effort in promulgating an aggressive "Defend Forward" posture in cyberspace.[14]

However, there are a few key points to consider as it relates to Israel's precedent. Hamas and Israel were already engaged kinetically, so an additional airstrike is not overly escalatory in nature. Additionally, further research still should be done to determine how effective Israel's actions were in deterring future Hamas cyber operations. Those points aside, the Israeli example may offer insights for future US actions. First, the US should have the mechanisms to conduct such a mission, practice it, and then publicize the results of the rehearsals. Second, the US should continue to advertise and execute its right to exercise sovereign options in cyberspace and update its various strategy and doctrine to reflect this position. The intent is to remove any ambiguity in where and how a cyberspace attack might warrant a response, lethal or nonlethal, much like in the traditional air, sea, or even land domains. In so doing, the US seeks to impose a new decision calculus to foreign actors.[15] Malicious cyber actors need to understand that cyber attacks, such as damaging or degrading US critical infrastructures (e.g., electrical control systems or bulk telecommunication networks), will be evaluated for equivalency to an attack on the US homeland. The evaluation could merit a violent, forceful response.

How could multidomain responses to a cyber attack work? There is a two-fold requirement that needs refinement and development in US government and DOD operating procedures and doctrine. First, by executing and publicizing its sovereign options in cyberspace, the US will continue setting norms on what types of assets, personnel, and other protected resources will trigger a response (e.g., the declaration of a national emergency up to and including a declaration of war) if attacked in cyberspace. Secondly, the US must resolve the attribution problem, namely the incontrovertible and unambiguous identification of cyber threat actors, including the infrastructure and information systems used by adversary cyber and APT forces. While attribution is no small feat, the US must invest and deploy resources to discover, to an acceptable degree of certainty, who is responsible for cyber attacks, including the geolocation of the attackers.

Additionally, the DOD, in coordination with interagency partners and the National Security Council, should incorporate kinetic response options to cyber attacks into existing strategies, plans, and rules of engagement (ROE) for all combatant commands in which threat actors reside. Engaging in "cyber diplomacy" is one immediate and potentially dividend-yielding activity that the DOD can employ. The DOD has well-developed expertise in cyber and network defense. Consequently, sharing this knowledge will help partner nations build out their defensive capabilities and enhance the US's alliances. Sharing cyber expertise will enable partners to detect and defend their networks, report and share adversary identifications, markers, and tactics, techniques, and procedures (TTP). It will also reduce the network surface through which an adversary can launch cyber attacks against US critical infrastructure.[16]

Specifying the type of malicious cyber activity that could trigger a forceful response is the first step in presenting a new value proposition to competitors in cyberspace. A starting point for the discussion could be the list of critical infrastructure identified in Presidential Policy Directive (PPD) 21, which lists 16 categories of interests that underpin US safety and national security.[17] This list leads to the second condition, for which there is no simple solution: how to accurately identify these APTs and threat actors and attribute their hostile activities to them.

How would the US go about identifying cyber threats and also resolve the nonrepudiation problem? As stated earlier, identifying the responsible party of a cyber attack presents an asymmetric challenge—attribution is often much more complicated than the effort required to obfuscate the source of the attack. The difficulties of attributing an attack are not just an issue in cyberspace. The attribution problem is common to several national security threats, namely transnational criminal networks (TCN) and terrorist networks. In fact, there are many similarities between APTs and terrorists and TCNs as evidenced by the table below.

Common properties	*Cyber threats and APTs*	*TCNs and terrorist networks*
Can be motivated by financial gain	GandCrab campaign generated $2 billion in revenue.[18]	Upon seizing Mosul, the value and assets Islamic State in Iraq and Levant ISIL seized was worth $2 billion.[19]
Disregard for rule of law and human suffering	For two years hackers/APTs targeted Ukrainian electrical infrastructure disabling power to thousands of customers.[20]	Cartel members overwhelming Government of Mexico forces and threatening violence to thousands of civilians in a bid to free cartel leader[21]
Operate in hostile countries, often tolerated	Russia is tolerating the participation of “Patriotic Hackers” during conflicts with its neighbors.[22]	The government of Sudan and the Taliban in Afghanistan allowing al-Qaeda to operate unchecked within their respective countries
Targets critical infrastructure/US military/allies	Consistently targeting US cities, federal agencies, and defense contractors	2019 attack on Saudi Arabian oil infrastructure[23]

Table. Common properties of cyber threats and APTs vs TCNs and terrorist networks

The likenesses between cyber threat actors and terrorist or criminal threats may be advantageous in that the doctrinal principals of counterterrorism may apply well to counter-APT efforts. Using Joint Publication (JP) 3-25, *Countering Threat Networks*, as a model, the identification of cyber threats and APTs would begin by conducting network analysis. This analysis will characterize the capabilities of a particular cyber threat or APT.[24] The next step is to conduct critical factors analysis, leading to the identification of adversary centers of gravity (COG), critical capabilities (CC), critical requirements (CRs), and critical vulnerabilities (CV).[25] As a notional example, a COG might be the command and control (C2) element or individuals associated with a threat, critical capabilities might be the attack and exploitation mechanisms a cyber-threat or APT might possess, a CR might be the network connectivity needed for a cyber threat or APT to initiate attacks, and a CV might be vulnerabilities within the TTPs that such a group might employ.

Just as the US does not tolerate the existence of threatening terrorist networks, neither should it tolerate the existence of cyber threat networks. From the *2018 Cyber Strategy*, persistent engagement means the US government (USG) and DOD should collaborate and coordinate the full spectrum of the intelligence community to employ human intelligence, signals intelligence, electronic intelligence, communications intelligence, and every other capability in between to discover and enumerate these networks. If a particular APT has a tactic or procedure to use virtual private networks, the onion routing network, or other mechanisms to hide their sources, it is imperative the intelligence community discover and monitor these sources and build up the technical capabilities to do so. If there is a particular school, website, or learning service that an adversary prefers to employ to train their cyber forces, the US must employ collection methods into these areas, not unlike having sources and insights into terrorist training camps and facilities.

Assuming the USG establishes and attribute the identities and actions of cyber threats or APTs, a next step is to employ the targeting cycle with deference to the desired effects on networks metrics of neutralize, degrade, disrupt, destroy, defeat, deny, or divert. Ultimately, this tactic could lead to outcomes of violent military force, such as bombing a building (e.g., the IDF airstrike on the Hamas cyber unit) or employing US Special Operations Command forces to capture or kill foreign cyber threat actors targeting US critical infrastructure.[26] Lastly, in order to fully exploit Total Force Integration, the expansion of Guard and Reserve intelligence and cybersecurity organizations and programs, such as the Joint Reserve Intelligence Centers (JRIC) or National Guard Cyber Protection Teams (CPT), should be explored as both could be a significant force and capability multiplier, especially if said Guard and Reserve members are placed in civilian cybersecurity roles within US critical infrastructure when on civilian status.[27] Suppose an incident response or security operations center analyst at an electrical utility was a Guard or Reserve member. He/she/they may then be trained to become familiar, or even expert, with some of the utility's control systems. This analyst may even be able to install and monitor CPT sensors on their utility's control network, assuming the technical, financial, and legal considerations can be overcome. In the event of compromise, the analyst could then start direct reporting information to the

Department of Homeland Security (DHS) and Cybersecurity and Infrastructure Security Agency (CISA), possibly having direct classified discussions, assuming the infrastructure is in place to do so. Subsequently, the analyst could immediately then get on voice orders, go to a JRIC, Guard CPT, or even an air operations center component like the Intelligence, Surveillance, Reconnaissance Division, and start adding expertise with an unprecedented level of insight into cyber or even kinetic targeting cycles. The analyst could aid in weaponeering and help in identifying the right affect against a particular target, given their intimate knowledge of the adversary TTPs being employed. Or the analyst could go to a Joint Targeting Board to articulate the type of effect a cyber threat or APT is having on their employer's control system network in order to increase targeting priorities. It is worth noting that the DHS already leverages programs like the Cyber Information Sharing and Collaboration Program and the EINSTEIN Project. These programs aid in information sharing, but figuring out and overcoming the necessary legal, jurisdictional, operational, and civil-military obstacles are also easier said than done to enable these cohesive, rapid, and full-range responses.[28] All of these steps would be essential for appropriate mission analysis in the Joint Operating Planning Process for Air.[29]

Using the above information as a backdrop, consider the following scenarios, steps of action, and responses. Cyber espionage against US election systems or cleared defense contractors (CDC) might warrant responses by legal means, including indictments by the Department of Justice. Still, cyber espionage to conduct the equivalent of Joint Intelligence Preparation of the Operating Environment (JIPOE) against US electrical, water, gas, telecommunication, and other critical infrastructure may need joint law enforcement or military response. In this case, if a utility detected and verified the Indications of Compromise (IOC) or TTPs from known APTs, the DHS and CISA could notionally be notified with the evidence of these IOCs and TTPs. These include relevant Internet Protocol or Media Access Control addresses, network traffic, email artifacts, system and event logs, login account audits, malware samples, and any other supporting information.[30] If the threat is determined to be sourced outside the jurisdiction of the US, then DHS and CISA should then liaise with DOD entities, such as the Defense Intelligence Agency and/or National Security Agency, to assist in determining the attribution of the cyber threat group. Again, this notification cycle might be shortened if there are Guard or Reserve members on civilian status employed as civilians within the cyber security organization of an affected utility. If the cyber threat group is based overseas, the combatant command responsible for the area in which the threat resides would perform standard targeting and planning processes, using established targeting guidance and JP 3-25 procedures.

If the foreign threat/APT furthers their compromise of a utility by moving beyond the JIPOE phase into manipulating or disrupting a utility's Human Machine Interfaces, Distributed Control System, or Supervisory Control and Data Acquisition system, forceful response actions, having been enriched by the intelligence generated by the aforementioned processes, could then be considered.

Given such a notional scenario, suppose that mission analysis concludes that malicious cyber actors, operating out of a multistory building (such as the facility mentioned that the IDF targeted), are determined to be responsible. Further, suppose that the building is within an area of responsibility of a combatant command where ROEs, for both kinetic and nonkinetic effects, already exist. If the building meets targeting guidance for the AOR, the facility is subject to target nomination. If the target is validated and vetted, the target may be added to the Joint Integrated Priority Target List, and, if consistent with the joint force commander's guidance, added to the air tasking order.[31] Mobile targets or targets that are time-sensitive, which is likely to be the case with many targets, would equally be susceptible to dynamic targeting (with its six distinct find, fix, track, target, engage, and assess [F2T2EA] steps), with the "fix" step the most involved in determining attribution.[32] After appropriate weaponeering, the target could be struck, either with conventional munitions or other military capabilities, from electronic warfare to Space-Enabled Cyber Operations to the employment of USSOCOM forces, all of which would be followed by standard battle damage assessment processes.

A principal sticking point of delineating the type of cyber intrusion, and who is responsible for responding, is an ongoing debate of legality. When does a cyber attack become a law enforcement matter versus one of national security concern to the US? When is a computer exploitation attack considered a case of espionage? Is it election hacking or the theft of sensitive or classified information? When is a cyber attack an act of war? Would it be an act of war for a cyber threat actor or APT to disrupt or degrade the utility or telecommunication service belonging to one of the critical sectors described in PPD 21? These are questions that combatant commanders should field to the Joint Staff and Office of the Secretary of Defense so that they can begin working with Congress and the national security enterprise to clear up the current state of ambiguity. If positive attribution to a cyber attack has been achieved, particularly in US Northern Command (USNORTHCOM) where the preponderance of the US critical infrastructure and homeland defense mission resides, what is the USNORTHCOM commander's, or any other impacted combatant commander's, roles and rights in inherent self-defense? What about liaising with USCYBERCOM, the Cyber National Mission Forces, and other supporting forces tasked with critical infrastructure protection? Until the theater ROEs are defined, CCDRs have little option but to absorb the blow and maintain a largely defensive posture. If ROEs were sufficiently mature, combatant command planners could instead start generating more active civil and military critical infrastructure defense-related flexible deterrence options and flexible response options per JP 5-0 *Joint Planning*.

Beyond the legal authorities and implications inherent in the homeland defense mission, international concerns also need to be addressed. Maj Gen Didier Tisseyre, commander of France's Cyber Defense Command, has several adroit observations about cyber defense and notes, "If an organization such as NATO is attacked, then France is, by principle, against collective attribution. . . You have to be able to prove it, and the state that has been blamed might not appreciate having the finger pointed at it."[33] Therein lies further discussion, particularly with US's North Atlantic Treaty Organization (NATO) allies about its views, the ROEs for when and how we would respond, and thus the ROEs for when and how we would invoke Article 5 of the NATO treaty for mutual defense against a cyber attack.

Although both policy changes and attribution present large hurdles, something must be done to unmask, and continually confront, cyber threats, APTs, and similar rogue actors. By not establishing bright lines and systematically identifying and targeting these adversary forces, and by not meting out "retribution," we allow "evil to continue." In times of crises and conflict, not only will we face the continuing taunts of threat groups like GandCrab unabated, we might have to do so under candlelight—if we even have connectivity at all at that point.[34] ✪

Maj Lou Nguyen, USAF

Major Nguyen is the deputy chief, Vulnerability Management Branch, J34, Joint Force Headquarters-DOD Information Network at Fort Meade, Maryland when he is on active status with the Air Force Reserve. Previously, he was deputy chief, Strategy Plans Division, 9th Combat Operations Squadron at Vandenberg AFB, California. In his private civilian career, he is the senior cybersecurity engineer for a large natural gas utility in the United States.

Lt Col Jeremy L. Sparks, USAF

Lieutenant Colonel Sparks is the commander, 333rd Training Squadron, Keesler AFB, Mississippi. Previously, he was the weapons and tactics branch chief and Joint Access Operations Center chief at US Cyber Command, Fort Meade, Maryland.

Notes

1. Joie Salvio, "GandCrab Threat Actors Retire. . . Maybe," *Fortinet Threat Research*, 24 June 2019, https://www.fortinet.com/.

2. Brian Krebs, "Who's Behind the GandCrab Ransomware?," *Krebs on Security*, July 2019, https://krebsonsecurity.com/.

3. The National Institute of Standards and Technology defines an *advanced persistent threat* as: "An adversary that possesses sophisticated levels of expertise and significant resources which allow it to create opportunities to achieve its objectives by using multiple attack vectors (e.g., cyber, physical, and deception)," https://csrc.nist.gov/.

4. Walter Isaacson, "How to Fix the Internet," *The Atlantic*, 15 December 2016, https://www.theatlantic.com/.

5. Garrett Hinck and Tim Maurer, "What's the Point of Charging Foreign State-Linked Hackers?," *LawfareBlog*, 24 May 2019, https://www.lawfareblog.com/; and Department of Justice, "Report of the Attorney General's Cyber Digital Task Force," July 2018, https://www.justice.gov/.

6. Curtis E. LeMay Center for Doctrine Development and Education, *Challenges of Cyberspace Operations*, in "Annex 3-12, Cyberspace Operations" (Maxwell AFB: Air University, 11 November 2011), https://www.doctrine.af.mil/.

7. Department of Defense (DOD), *Department of Defense Strategy for Operating in Cyberspace,* July 2011, https://apps.dtic.mil/.

8. DOD, *Summary: Department of Defense Cyber Strategy*, 2018, https://media.defense.gov/.

9. Ellen Nakashima, "U.S. Cyber Command Operation Disrupted Internet Access of Russian Troll Factory on Day of 2018 Midterms," *Washington Post*, 27 February 2019, https://www.washingtonpost.com/.

10. Nakashima, "U.S. Cyber Command Operation Disrupted Internet Access."

11. David Alexander, "U.S. Reserves Right to Meet Cyber Attack with Force,*" Reuters Technology News*, 15 November 2011, https://www.reuters.com/.

12. Twitter's account of the Israel Defense Forces: "CLEARED FOR RELEASE: We thwarted an attempted Hamas cyber offensive against Israeli targets. Following our successful cyber defensive operation, we targeted a building where the Hamas cyber operatives work. HamasCyberHQ.exe has been removed," 5 May 2019, https://twitter.com/.

13. Elias Groll, "The Future Is Here, and It Features Hackers Getting Bombed," *Foreign Policy,* 6 May 2019, https://foreignpolicy.com/.

14. US Cybersecurity Solarium Commission, March 2020, 23–25, https://www.solarium.gov.

15. David Sanger and Nicole Perlroth, "U.S. Escalates Online Attacks on Russia's Power Grid," *New York Times*, 15 June 2019, https://www.nytimes.com/.

16. Dr. Panayotis A. Yannakogergos, "Strategies for Resolving the Cyber Attribution Challenge" (Maxwell AFB, Air University: May 2016), 58–59; and U.S. Cybersecurity Solarium Commission, 2–7.

17. Presidential Policy Directive 21, *Presidential Policy Directive—Critical Infrastructure Security and Resilience*, 21 February 2013, https://obamawhitehouse.archives.gov/.

18. James Walker, "GandCrab Closure Will Lead to 'Power Vacuum' in Ransomware Market," *Daily Swig,* 20 June 2019, https://portswigger.net/.

19. Martin Chulov, "How an Arrest in Iraq Revealed Isis's $2bn Jihadist Network," *The Guardian*, 15 June 2014, https://www.theguardian.com/.

20. Darren Pauli, "Crims Shut off Ukraine Power in Wide-Ranging Anniversary Hacks," *The Register*, 12 January 2017, https://www.theregister.co.uk/.

21. Will Grant, "Mexico's Bid to Detain El Chapo Son 'a Failure of Everything,'" *BBC News*, 18 October 2019, https://www.bbc.com/news/.

22. Michael Connell and Sarah Vogler, "Russia's Approach to Cyber Warfare," *Center for Naval Analyses*, March 2017, 13; and Scott D. Applegate, "Cybermilitias and Political Hackers: Use of Irregular Forces in Cyberwarfare," *IEEE Security and Privacy* 9, no. 5 (September 2011): 16–22.

23. Michael Safi, "Iran Denies Launching Drone Attacks on Saudi Oil Facility," *The Guardian*, 15 September 2019, https://www.theguardian.com/.

24. Chairman of the Joint Chiefs of Staff (CJCS), *Joint Publication (JP) 3-25 Countering Threat Networks* (Washington, DC: Department of Defense, 21 December 2016), II-1–III-9, https://www.jcs.mil/Portals/; and Mitre, "Groups," https://attack.mitre.org/.

25. CJCS, *JP 3-25, Countering Threat Networks* (Washington, DC: Department of Defense, 21 December 2016), IV-4, https://www.jcs.mil/Portals/.

26. CJCS, JP 3-25, V-1–V-16.

27. David Vergun, "Reserve, Guard Leaders Provide Cybersecurity Updates," 26 March 2019, https://www.defense.gov/.

28. Department of Homeland Security (DHS), "Cyber Information Sharing and Collaboration Program (CISCP), 23 November 2015, https://www.cisa.gov/, and DHS, "Einstein," 21 August 2015, https://www.dhs.gov/cisa/einstein.

29. Curtis E. LeMay Center for Doctrine Development and Education, *The Joint Operation Planning Process for Air*, in "Annex 3-0, Operations and Planning" (Maxwell AFB, AL: Air University, 4 November 2016), https://www.doctrine.af.mil/.

30. Danny Bradbury, "Iran's APT33 Sharpens Focus on Industrial Control Systems," 22 November 2019, https://nakedsecurity.sophos.com/.

31. Curtis E. LeMay Center for Doctrine Development and Education, *Contingency and Crisis Execution: The Tasking Cycle*, in "Annex 3-0, Operations and Planning" (Maxwell AFB, AL: Air University, 4 November 2016), https://www.doctrine.af.mil/.

32. Curtis E. LeMay Center for Doctrine Development and Education, *Dynamic Targeting and the Tasking Process*, in "Annex 3-60, Targeting" (Maxwell AFB, AL: Air University, 15 March 2019), https://www.doctrine.af.mil/.

33. Christina Mackenzie, "France's New Cyber Defense 'Conductor' Talks Retaliation, Protecting Industry," *Defense News*, 30 September 2019, https://www.fifthdomain.com/.

34. Kelly Jackson Higgins, "Latest Ukraine Blackout Tied to 2015 Cyberattackers," *Dark Reading,* 10 January 2017, https://www.darkreading.com/.