

The Cyber Collective Threat

A Pack of Lone Wolf Terrorists

Max | Sterling



Brief No. 9.6

The Project on International Peace and Security © 2017
All rights reserved.

Please direct inquiries to:
The Project on International Peace and Security (PIPS)
Institute for the Theory and Practice of International Relations
The College of William and Mary
427 Scotland Street
Williamsburg, Virginia 23185
tele. 757.221.1441
fax. 757.221.4650
pips@wm.edu

Electronic copies of this report are available at www.wm.edu/pips

The Project on International Peace and Security

Launched in 2008, the Project on International Peace and Security (PIPS) is an undergraduate think tank based at the College of William and Mary. PIPS represents an innovative approach to undergraduate education that highlights the value of applied liberal arts training to producing the next generation of foreign policy analysts, leaders, and engaged citizens.

PIPS is premised on two core beliefs: (1) rigorous policy-relevant research is a core component of a student's education; and (2) when guided by faculty and members of the foreign policy community, undergraduates can make meaningful contributions to policy debates; their creativity and energy are untapped resources. To this end, PIPS each year selects six research fellows and six research interns. Research fellows identify emerging international security challenges and develop original policy papers. Research interns support the work of the fellows and learn the craft of conducting policy research and writing briefs.

For more on PIPS, visit www.wm.edu/pips.

Amy Oakes
Dennis A. Smith
Co-directors

The Cyber Collective Threat A Pack of Lone Wolf Terrorists

APRIL 2017

Max Sterling

The Cyber Collective Threat

A Pack of Lone Wolf Terrorists

Counterterrorism strategies often focus on the structure of terrorist groups, among other variables, to identify and exploit vulnerabilities within those organizations. Terrorist organizations generally range between centralized hierarchical structures to decentralized networks. The cyber world, however, enables the emergence of a structure outside the traditional view: the decentralized, lack-of-command “cyber collective.” This structure has the potential to enhance the resilience of terrorist organizations, increase the frequency of lone wolf terrorist attacks, and reduce the efficacy of targeting high value individuals. The cyber collective represents an unorthodox structure that has yet to be fully realized by a terrorist organization, but some of the actions and tactics of the Islamic State and Anonymous reflect the dangerous potential of this organizational structure.

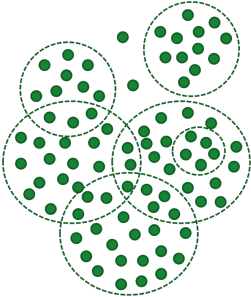

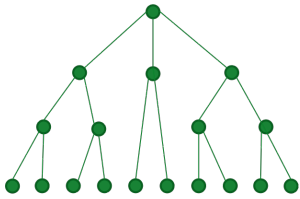
Introduction

The cyber world enables the cyber collective, a resilient and decentralized structure that lacks a strict chain of command and deliberate planning. This organization poses serious challenges to counterterrorism efforts, which rely on the targeting of leadership among other important factors to disrupt terrorists’ operations and destroy their organization. Should the Islamic State and other terrorist groups adopt the cyber collective structure, they could mobilize lone wolves to conduct attacks abroad or develop a robust safety net should traditional counterterrorism strategies weaken the group. The hacker collective Anonymous demonstrates the power of a cyber collective. A version of Anonymous with more destructive goals and clearer political motivations would represent an unpredictable danger to international peace.¹ Future terrorist groups will reap the benefits of the cyber world, so examining the cyber collective is crucial to fighting future terrorist organizations.

Traditional Organizational Structures: Hierarchies and Networks

The leadership structures of terrorist groups generally range from strict hierarchies to deconstructed networks (see Table 1). The clear chain of command in a hierarchy provides control of the organization, which allows the group to govern land and conduct complex attacks. Networks, which lack the rigidity of a hierarchy, have greater resilience and more global reach; however, they do not possess the command and control to hold territory or execute large-scale operations.

Table 1: The Cyber Collective, Network, and Hierarchy

	CYBER COLLECTIVE	NETWORK	HIERARCHY
<i>Recruitment</i>	Open	Formal	Formal
<i>Structure</i>	Circles with overlapping membership	Cells with covert, distinct branches	Cells with pyramidal structure
<i>Command</i>	Catalysts	Decentralized	Centralized
<i>Attacks</i>	Swarming, wolf pack, lone wolf attacks	Swarming attacks, enabled attacks by single branches, lone wolves outside network	Coordinated attacks, lone wolves outside hierarchy
			

Centralized Hierarchies

Hierarchies use a vertical chain of command through which clear orders flow from the centralized leadership at the top of the chain down to the lowest-level soldier.² The division of the organization allows cells to specialize in areas such as intelligence, support, or operations.³ The hierarchy enables coordinated operations and territorial control, but exposes the organization to counter-leadership targeting.⁴

- *Low resilience.* The pyramidal structure of hierarchies creates vulnerable organizations. Counter-leadership targeting can eliminate the apex of the pyramid, leaving the organization with a less competent leader.⁵ Further targeting leaves the hierarchy with a dysfunctional chain of command and weak centralized leadership and ultimately leads to the implosion of the organization.⁶
- *Strict command and control.* Within a hierarchy, centralized leadership issues orders, which allows strict control of the organization. As Brafman and Beckstrom describe, “power and knowledge are centralized at the top,” and without the centralized

headquarters the organization cannot function.⁷ Although the streamlined chain of command limits flexibility on the part of subordinates within the organization, governing bodies favor bureaucratic hierarchies. An organization needs a central decision-making body and a pyramidal structure beneath to execute tasks. The hierarchical structure also divides roles and responsibilities, forming specialized departments.⁸ This division allows the organization to perform diverse tasks and undertake large, complicated operations, but the specialization also makes every department critical.⁹ By disrupting one part of the hierarchy, the entire organization can be crippled.

- *Localized, political motivations.* Terrorist organizations with aspirations to hold or govern territory—such as the Islamic State within Syria and the Taliban in Afghanistan—employ a hierarchy.¹⁰ These groups are often localized, political, and linked specifically to separatist or nationalist terrorists.¹¹ Hierarchies may also be linked to religious ideologies, but specific political aspirations remain the primary driver. Although the hierarchy enhances the central leadership’s control, recruitment can be limited without the broad appeal of an issue.

Targeting key leadership can damage centralized hierarchies. However, the hierarchy appeals to local groups that aspire to hold land and govern territory. Because of this structure’s division of responsibilities, the organization can fulfill the many services necessary to control and govern territory.

Decentralized Networks

According to Arquilla and Ronfeldt’s characterization, the cells within a network are “diverse, dispersed ‘nodes’ who share a set of ideas and interests and who are arrayed to act in a fully internetted ‘all-channel’ manner.”¹² The decentralized nature of a network greatly enhances resilience and allows for a more global reach than a hierarchy, but the network less effectively governs and holds territory than a hierarchy.

- *High resilience.* Arquilla and Ronfeldt contend that, “networks tend to be redundant and diverse, making them robust and resilient in the face of an attack.”¹³ While the hierarchy can be significantly damaged by counter-leadership strikes, the network’s decentralized command can withstand targeted attacks on leadership.¹⁴ Additionally, Arquilla and Ronfeldt observe that the network may “absorb a number of attacks on distributed nodes, leading the attacker to believe the network has been harmed...when, in fact, it remains viable and is seeking new opportunities for tactical surprise.”¹⁵ The network is therefore resilient to targeted attacks both on individual leaders or commanders and on entire sections of the network itself.
- *Limited command and control.* Instead of providing specific direction and clear commands for subordinates, the network’s cells operate independently, often following the commander’s intent to make decisions.¹⁶ Audrey Kurth Cronin characterizes these organizations as “mission-driven,” they function through the intent of superiors, emphasize individual initiative, and lack “traditional logistical trails.”¹⁷ In this way, the

mission-driven network gives flexibility to subordinates, but may lose the potential to conduct complex attacks. Although largely mission-driven, the network retains a certain degree of true command. Whereas the hierarchy can use its combined power to plan, prepare, and execute complicated attacks, the network's ability to conduct such operations relies on coordinating between autonomous branches of the network. The branches of the network can collaborate to conduct swarming attacks, what Arquilla and Ronfeldt define as a "deliberately structured, coordinated, strategic way to strike from all directions at a particular point or points."¹⁸

- *Transnational, social or religious motivations.* Unlike the hierarchy, which is strongly linked by a strict command structure, the network relies on the strength of its ideology. Transnational groups often organize around religious or social ideologies, not political ideologies that are tied to a particular government.¹⁹ Therefore, this structure is common among transnational actors, such as al-Qaeda. According to Arquilla and Ronfeldt, "[the network] tends to defy and cut across state boundaries, jurisdictions, and distinctions between state and society, public and private, war and peace, war and crime, civilian and military, police and military, and legal and illegal."²⁰ The transnational reach of the network limits the methods available and complicates effort to discern legitimate and illegitimate action by both the network and its adversary.

Networks diminish the effect of targeting operations. Subordinates have a greater degree of autonomy and flexibility, which makes networks harder to predict and preempt than hierarchies. Networks also tend to be transnational and linked to religious or social ideologies, which blurs the line between legitimate and illegitimate action.

Cyber Collective Structure

In fact, the success of Anonymous without leaders is pretty easy to understand—if you forget everything you think you know about how organizations work.

-Quinn Norton, 2012²¹

The cyber collective is distinct from the network and hierarchy in three ways. First, the cyber collective has an open membership policy, instead of a deliberate system of recruitment and training. Second, coordination and communication overlap among the circles and the organization lacks any permanent, centralized command. Third, the attacks require little coordination, and include swarming attacks conducted by many circles, wolf pack attacks by a single circle, and lone wolf attacks by individuals.

Open Membership

Unlike the recruitment and training process of the Islamic State, the cyber collective does not deliberately recruit followers. Ryan Pereira outlines the Islamic State's recruiting process, tracing "potential targets from first contact with the group, through careful pruning of their social

networks, before culminating in a call to action on behalf of Islamic State.”²² This strategy creates an insulated network and attempts to shield the organization from infiltration. Carefully curating of the network guards against the recruitment of unworthy candidates. This strategy also ensures that calls to action fit the recruits.²³ The cyber collective has a riskier recruitment process. Members volunteer and most people use pseudonyms or remain anonymous online. The absence of deliberate recruitment creates a diversity of membership, strategy, experience, and ambition, which makes the collective unpredictable and difficult to disrupt. Identifying a recruitment pattern becomes far more difficult, and the open-door membership with limited vetting increases the likelihood a truly innovative, inspirational leader will join the organization.

Circles and Catalysts, not Cells and Commanders

Circles with overlapping membership conduct all-in, peer-to-peer communication. And catalysts—influential leaders—temporarily spur action within or between circles. One leader in a circle or one circle in the broader organization may play the pivotal role in one operation, but future operations will rely on different catalysts or different circles.

- *Circles.* In hierarchies, information flows up and down a vertical chain. And in networks, information can flow both horizontally through chains, hubs, or all-in channels and vertically from the top leadership to the edges of the network. In a collective, however, information travels directly between individuals to other members or the group at large, regardless of their standing within the organization.

Circles in the collective conduct all-in communications where members often simultaneously contact all other members of the circle, and no one person issues orders or commands.²⁴ The circles have overlapping roles and membership, and conduct similar, competing, or coordinated operations. Each circle has its own direction and catalysts, and circles can become rivals, divide to form new circles, or merge. Fluid communication exists between different circles, and the boundaries between circles can be unclear. Whereas a network remains covert, many circles in the collective are open and overt.

The hacker group Anonymous operates as a cyber collective with various circles whose membership overlaps. Some of these circles focus on specific operations of Anonymous—for example OPTunisia during the Tunisian revolution—while others have no specific purpose and participate in many different campaigns. Gabriella Coleman, an anthropologist who gained access to some Anonymous circles, found that “the entire AntiSec core team would sometimes work in unison, but more typically they splintered into smaller groups for different operations.”²⁵ Although she describes how one circle conducted his operations, she notes she had no knowledge of how other groups conducted similar or parallel operations.²⁶ Anonymous’s overlapping membership and redundant responsibilities demonstrate added resilience from the cyber collective.

- *Catalysts.* Leaders within circles leverage individual influence into action, serving as catalysts and then returning to the role of regular member. As Brafman and Beckstrom explain, “a catalyst gets a decentralized organization going, and then cedes control to the

members.”²⁷ Whereas Brafman and Beckstrom describe the catalyst as present only at the start of the organization, the collective survives through continued use of catalysts who spur the creation of circles, direct the circle’s action, and then step back into normal membership.

Anonymous is the closest to a true example of a cyber collective, although it is not a terrorist organization. Coleman documents how Sabu, a catalyst within Anonymous turned FBI informant, had a significant impact on many different Anonymous circles and operations, but “did not actually mastermind the operations or bark orders.”²⁸ Coleman contends that many journalists make the mistake of attempting to identify a “leader” or “mastermind” of Anonymous, when in reality the group tends to be dynamic and fluid, with multiple individuals or even groups working in concert.”²⁹

The cyber collective’s circles and catalysts encourage a flexible organization and increase its resilience. Catalysts wield their influence to create a circle or inspire action, but these leaders do not hold permanent power. Circles overlap, compete, and coordinate to conduct operations, so that no single leader or circle is critical to the operations of the cyber collective.

Low-Coordination Attacks

The cyber collective can conduct three types of attacks, which require less coordination than the attacks of a network or hierarchy. The cyber collective is a fully mission-driven organization and does not have commanders issuing orders because there are neither commanders nor subordinates in the conventional sense.³⁰ Attacks can arise from one inspired member or low-level coordination within or between circles.

- *Swarming attacks.* Swarming attacks occur when different parts of a network deliberately strike the same point, so these operations require significant coordination among circles.³¹ The cyber collective does not have the same level of secrecy as a network, and therefore requires far less coordination to conduct swarming attacks between overlapping circles. The overlapping membership also facilitates coordination between circles. Of the three attacks conducted by the cyber collective, the swarming attack is easiest to detect and preempt because it requires the most coordination. These attacks will most likely occur less frequently than wolf pack or lone wolf attacks, but the combined power and cumulative effect of the different circles create the potential for greatest damage.
- *Wolf pack attacks.* The rapport among members of a single circle makes coordination easy, and in practice attacks resemble lone wolf attacks. The mission of the organization, not commands, inspires wolf pack attacks.³² The combined power of the circle could make wolf pack attacks more damaging than attacks launched by a single member, and similar to the unpredictability of a lone wolf attack, the wolf pack coordinates so little that attacks will be difficult to detect and disrupt. The open communication within the circle will make wolf pack attacks more inventive, creative, and dangerous than the lone wolf attacks. Competition between different circles could also yield increasingly

ambitious operations, and without a centralized leadership limiting the risk subordinates assume, wolf pack attacks will be increasingly bold.

- *Lone wolf attacks.* The cyber collective encourages individuals to conduct independent lone wolf attacks, even if other members of the collective may disagree with the specific strategy. Similar to wolf packs, lone wolves will be bold and dangerous. However, whereas a circle has many individuals who debate the relative merits of different plans, the individual does not necessarily conduct the same thorough calculation of risk and reward, and could therefore be careless and not as well planned as wolf pack attacks. Lone wolves represent the most difficult type of attack to detect and preempt. Lone wolves, however, may not be able to conduct attacks as damaging as those by wolf packs or swarms.

The three characteristic attacks of the cyber collective are unpredictable and will be difficult to detect. Swarming attacks that require coordination between circles will be easiest to reveal, but benefit from greatest numbers of attackers. Lone wolves will be most difficult to discover and disrupt and the least risk-averse. Wolf pack attacks conducted by a circle will be similarly difficult to detect, and can capitalize on the entire membership of the circle to cause more damage than lone wolves.

Capacity in which Cyber Collectives Arise

Terrorist organizations can adopt the cyber collective structure at different points during their lifespan based on their capabilities, goals, and strength. For instance, an organization without aspirations to become a traditional organization could exist solely in the form of a cyber collective. Newly formed organizations could begin a traditional Maoist insurgency online—establishing political bases, bolstering support, and conducting asymmetric operations almost entirely in the cyber world—before moving into the physical world to fight a conventional insurgency. A strong terrorist organization could broaden its reach and build a strong foundation for the future by developing a cyber collective. Lastly, an organization weakened by counterterrorism could be forced into the cyber collective structure.

Pure Cyber Collective

A pure cyber collective is an organization with broad goals that can be transnational. These organizations never aspire to control land or govern territory. Instead, they exist only in the cyber world for the entirety of their existence. As a result, the fight against these terrorists occurs solely in the cyber world, which limits the counterterrorism tools available. The pure cyber collective inspires lone wolf attacks and disseminates propaganda that reaches a global audience, but also conducts coordinated cyber swarming attacks. The organization's cyber presence makes it difficult to map and disrupt, and ultimately this new threat will be a resilient and potent one. Anonymous represents a pure cyber collective—an organization that does not aspire to organize

beyond the Internet. This manifestation of the cyber collective, however, may be the most dangerous because of the limited options to fight this organization.

First Phase for an Emerging Insurgency

Mao Tse-Tung describes the phases of an insurgency, which moves from the rural, guerrilla first and second phase to the third phase, during which the insurgent regains territory.³³ An emergent insurgency could organize its first phase using the Internet to build support for its cause and conduct asymmetric cyber attacks on its enemy. This organization would have the advantage of existing solely online, and could therefore mobilize membership globally while evading counter offensives. As the insurgents win victories and transition to conventional organizations and operations, they could maintain the cyber collective as a fallback option and become a comprehensively resilient organization. The first phase insurgent would begin with lone wolf or wolf pack attacks, and as it progresses past the first phase could conduct more coordinated swarming attacks. Similar to the logic of guerilla warfare, the first phase cyber collective could capitalize on strategic surprise and boldness to win early victories, and through online propaganda the insurgency could broaden its base of support.

Retrenchment Strategy for a Weak Organization

As counterterrorism efforts weaken traditionally organized hierarchies or networks, a terrorist group could be forced reorganize as a cyber collective in order to survive. By continuing to communicate and plan future operations through the Internet, the reeling group can recoup and develop a strategy for long-term success. Once the group has sufficiently recovered, the organization could return to a traditional hierarchy or network. Like the insurgent advancing from the first phase cyber collective, the recovered organization preserves the cyber collective, which can provide support and resilience in the future.

For example, the Islamic State (IS) has been forced to adopt more decentralized structures as counterterrorism efforts force IS underground. As these operations continue, the Islamic State may organize using the cyber collective until it has won enough victories, effectively reshaped the narrative, or increased membership to the point that the organization could pursue its broader goals through a centralized structure.

Safety Net for a Strong Organization

A strong group could include a cyber collective element, capitalizing on their strong position to produce propaganda that supports a winner's narrative. In this way, the cyber collective can build a propaganda strategy and attract new members while the organization is in a position of strength. This strategy would create a fallback option that would ensure the ultimate survival of the organization should the group experience a series of failures.

Implications for Counterterrorism

It's one of the great paradoxes of our time that the very technologies that empower us to do great good can also be used to undermine us and inflict great harm.

—President Barack Obama, 2015³⁴

The nature of the cyber collective—its recruitment, structure, and attacks—produce challenges for counterterrorism efforts. First, the catalysts and circles in the collective decrease the efficacy of counter-leadership targeting, making the organization more resilient. Second, the speed of communication in the cyber collective enables innovative and potent attacks that come with little prior warning. Third, the cyber world blurs the lines between legal and illegal action and between combatants and non-combatants.

Ineffectiveness of Counter-leadership Targeting

For every circle eliminated, new circles form and learn from the previous circle's mistakes. Countering the collective using targeting operations such as drone strikes or Special Forces raids would be useless against an online organization. Should counterterrorism strategies dismantle a circle, the remnants could form many new circles. Similarly, the lack of a centralized leader or commander weakens targeting operations. Targeting a catalyst, a leader with temporary influence, would have a limited impact on the organization on the whole.

Attempts to target Anonymous's structure or limit their access to the Internet have demonstrated the challenges of combatting the collective. In Britain, the Government Communications Headquarters (GCHQ) launched massive denial of service attacks on Anonymous and collected large-scale surveillance on cyber communications.³⁵ Coleman reports how these counter cyber attacks did little to disrupt Anonymous's operations and the majority of the surveillance collected came from normal citizens without involvement in Anonymous.³⁶

Problem of Detecting Attacks

Bolstering defenses, detecting an impending attack, or preempting an operation will prove difficult due to covert cyber communication and the speed of communicating online. The decentralized operations and open membership encourage combatants to conduct attacks that play to their strengths and will produce inventive and daring operations. Attacks can be planned and executed quickly with limited consideration of risk. Fractures and disagreements between different circles produce competition, which leads to increasingly ambitious and dangerous attacks.

Challenges of jurisdiction and distinguishability

Defining legitimate versus illegitimate action online proves difficult. What constitutes an attack, and who should be labeled a combatant? Similarly, determining which internal agency, country,

or international organization should lead the fight could be challenging, and jurisdiction issues could slow the process of countering the collective. The options available to combat an online organization raise questions about the right to privacy and assembly online, as well as the role of the international community in cyber policing

For example, the cyber security firm HBGary attempted to use social media to unmask members of Anonymous, and the ensuing conflict between the two organizations highlights the challenge of online distinguishability.³⁷ Through a series of destructive hacks, Anonymous revealed HBGary's misinformation and humiliated the firm and its key players. Coleman writes the hackers "quickly noticed innumerable mistakes. Many of the named individuals had done nothing illegal."³⁸ This incident demonstrates one of the greatest challenges in fighting a cyber organization—discerning between legal and illegal actions. Beyond these mistakes, Coleman notes that the "most glaring problem was [HBGary's] ignorance of the key operatives behind this very hack."³⁹ Although HBGary tried to map Anonymous, the firm actually missed the most important players of the organization, and the information they did uncover could have been learned from public sources.⁴⁰

Any cyber organization presents challenges in discerning between legal and illegal operations and between combatants and non-combatants. But the cyber collective creates a deeper problem: the immense difficulty of first correctly mappings and then dismantling the organizational structure.

Strategies to Fight the Cyber Collective

The United States, along with its counter terrorism allies, can employ several strategies to exploit the cyber collective's vulnerabilities. First, challenging the cyber collective's message can stunt recruitment, blunt attacks, and dissuade would-be lone wolves from taking action. Second, directly disrupting the recruitment process will force the organization to become more stratified and to adopt formal vetting processes, which will make the collective less bold and more predictable. Third, slowing the operational pace by pushing the organization towards traditional structures will lessen the threat of attack and undercut the winner's narrative, impeding further recruitment.

Challenge the Message

The mission-driven nature of the cyber collective creates a reliance on messaging and communication, both to draw in new members and inspire action after the organization has formed. Fighting the message of the cyber collective can prevent autonomous attacks and dissuade people from joining the organization. Members will want to join an organization that they believe in and which has won victories. Limiting or countering the cyber collective's propaganda can challenge the "winner's narrative" of the organization.⁴¹ Not only will this strategy discourage recruitment, it will also preempt lone wolves by taking away much of the inspiration for conducting an attack. The platforms through which the

cyber collective operates and organizes provide opportunities for counter messaging campaigns through one-on-one communications, videos, articles, or other pop-ups.

Alternatively, capitalizing on the open membership policy and encouraging in-fighting among the organization's members can cast doubt on the message. By exploiting rivalries between circles, highlighting ideological differences between branches of the organization, or suggesting ludicrous or extreme action, members will be forced to question their belief in the mission of the organization. The more a member debates, doubts, or disagrees with the mission of the organization, the less likely that person will be to take action. The same tactic can apply to the operations the cyber collective undertakes—a counter-collective strategy that encourages debate about appropriate methods could limit the collective's bold actions, make the organization more predictable, and prevent some individuals from conducting autonomous operations.

Disrupting the Recruitment Process

Open membership provides another opportunity to disrupt the cyber collective by influencing the recruitment process. The self-selection process of the organization will not hold up should many new recruits be proven to be non-believers. Flooding the organization with fake members—whether through real agents or bots—can force the organization to vet its members earlier in the process. Further vetting will limit the diversity of the organization and slow operations. Overloading the cyber collective with new members will also force the organization to stratify. As members must prove or define their role and utility within the organization, the cyber collective will look more like a centralized hierarchy or a network, and can therefore be targeted more easily. On a larger scale, driving a wedge between different circles can stratify the organization further and force recruitment to become slow and deliberate. The greater the barriers to enter the cyber collective, the more predictable and conventional the organization will become. Over time, slowing or complicating the cyber collective's recruitment will funnel the organization into traditional recruitment and command structures, which make the crippled cyber collective far easier to target and topple.

Slowing Operations

One of the cyber collective's greatest advantages lies in its speed of organization and operation. Extensive debate about ideology or appropriate methods can slow the organization—time spent debating and doubting the message and methods is time that could have been spent acting. Flooding the organization with members and forcing the collective to stratify can also lower the operational pace. Stratifying the cyber collective pushes the organization towards more conventional command structures, whose members think more carefully about risk, carefully plan operations, and receive confirmation from higher levels before carrying out an operation. Together these factors considerably slow the cyber collective and also eliminate victories necessary to fuel a winner's narrative throughout its messaging. The cyber collective's most dangerous attacks are bold, come with little warning, and will be quickly followed by subsequent attacks; operations that take more time to be

executed will be more predictable, more likely to be detected and preempted, and will have a greater lull before the next attack. In this way, slowing operations not only lessens the overall threat of attacks, but also takes away the victories needed to sustain the narrative that attracts members and inspires individual action.

Conclusion

The cyber collective exists outside the conventional view of terrorist organizational structure, which views these groups as ranging from hierarchies to networks. The cyber collective, however, has no centralized leadership or chain of command, clearly designated cells, or deliberate planning in establishing the organization. Instead, the cyber collective relies on catalysts to spur action among circles with overlapping responsibilities and membership, and is a mission-driven organization that empowers subordinates to act autonomously. The cyber collective therefore represents a resilient organization that will conduct bold, unpredictable lone wolf and wolf pack attacks.

Cyber collectives also apply to a variety of different types of terrorist groups. Like Anonymous, an organization could never seek to exist in the physical world or govern territory. An insurgent could use the cyber collective as its first phase of insurgency, establishing political bases and gaining membership online. And both weak organizations reeling from counterterrorism strategies as well as strong organizations looking to create a safety net could use the cyber collective as a fallback option. The cyber world enables the emergence of this dangerous, unpredictable threat.

Future strategies could exploit some key variables of the cyber collective in an effort to challenge the organization's message, disrupt its recruiting process, and slow its operational pace. However, as organizations learn more about how the cyber world can be used to enhance their organizations, the threat of a cyber collective grows. Studying the implications of the cyber collective can prepare the United States for the threat of future cyber-enabled terrorist groups.

¹ This paper does not intend to provide a normative statement about Anonymous, its operations or ideology. Rather, this paper provides a description of the unique collective structure present in Anonymous, and subsequently imagines the potential challenges of facing a constructed with a similar structure.

² U.S. Army Training and Doctrine Command, "Terrorist Organizational Models," in *A Military Guide to Terrorism in the 21st Century: DCSINT Handbook No. 1*, (TRADOC, 2007), accessed October 28, 2016, <http://www.au.af.mil/au/awc/awcgate/army/guidterr/ch03.pdf>, 3-6.

³ TRADOC, "Terrorist Organizational Models," 3-6.

⁴ David Arquilla and Jon Ronfeldt, "The Advent of Netwar," in *Networks and Netwars*, ed. David Arquilla and Jon Ronfeldt, accessed December 12, 2016, http://www.rand.org/content/dam/rand/pubs/monograph_reports/MR1382/MR1382.ch1.pdf, 8; Additionally, networks can be linked to a hierarchy or many networks can be organized into a hierarchy. As Arquilla and Ronfeldt note, "traditional hierarchies may exist inside particular nodes in a network," or else "some actors may have a hierarchical organization overall but use network designs for tactical operations."

⁵ Brafman and Beckstrom, *The Starfish and the Spider*, (New York: Portfolio, 2006), 143; Dan Byman, "Do Targeted Killings Work," *Foreign Affairs*, (March/April 2006 Issue), accessed March 26, 2017, <https://www.foreignaffairs.com/articles/israel/2006-03-01/do-targeted-killings-work>; This targeting could in fact have the opposite effect. Eliminating weak leaders from the organization could leave the organizations with the most competent leaders, or could spark retaliation from the targeted organization. In the cyber collective, targeting leadership would have multiple impacts. Targeting leadership will ultimately be ineffective against an organization with no true command. However, attempting to target leadership or even targeting individual circles or members will certainly spark the retaliatory effect that Byman outlines; Anonymous's response to HBGary's attempt to map Anonymous's organizational structure demonstrates the potentially damaging impact of targeting the cyber collective.

⁶ Brafman and Beckstrom, *Starfish and Spider*, 143.

⁷ Brafman and Beckstrom, *Starfish and Spider*, 49; Brafman and Beckstrom note how, "centralized organizations depend more on structure, and that tends to make them more rigid."

⁸ Brafman and Beckstrom, *Starfish and Spider*, 50.

⁹ Brafman and Beckstrom, *Starfish and Spider*, 50.

¹⁰ Cameron Glen, "Al-Qaeda vs. ISIS: Leaders and Structure," *Wilson Center*, last modified September 28, 2015, accessed February 14, 2017, <https://www.wilsoncenter.org/article/al-qaeda-v-isis-leaders-structure>; ISIS has not always employed a hierarchical structure, and especially now given ISIS's waning power it increasingly employs decentralized command structure. However, as this article documents, the Islamic State has a more extensive pyramid bureaucracy.

¹¹ U.S. Army Training and Doctrine Command, "Terrorist Motivations and Behaviors," in *A Military Guide to Terrorism in the 21st Century: DCSINT Handbook No. 1*, (TRADOC, 2007), accessed October 28, 2016, <http://www.au.af.mil/au/awc/awcgate/army/guidterr/ch02.pdf>, 2-5.

¹² Arquilla and Ronfeldt, "Advent of Netwar," 7.

¹³ Arquilla and Ronfeldt, "Advent of Netwar," 13.

¹⁴ Ibid.

¹⁵ Ibid.

¹⁶ Audrey Kurth Cronin, "How al-Qaeda Ends," *International Security* 31 No. 1 (2006), 13.

¹⁷ Cronin, "How al-Qaeda Ends," 13.

¹⁸ Arquilla and Ronfeldt, "Advent of Netwar," 12.

¹⁹ TRADOC, "Terrorist Motivations and Behaviors," 2-8.

²⁰ Arquilla and Ronfeldt, "Advent of Netwar," 14.

²¹ Quinn Norton, "How Anonymous Picks Targets, Launches Attacks, and Takes Powerful Organizations Down," *Wired*, (July 3, 2012), accessed October 28, 2016, https://www.wired.com/2012/07/ff_anonymous/.

²² Ryan Pereira, "The Islamic State's Social Media and Recruitment Strategy: Papering Over the Flimsy Caliphate," *Georgetown Security Studies Review* 4, No. 1 (January 2016), accessed January 12, 2017, <http://georgetownsecuritystudiesreview.org/wp-content/uploads/2016/01/GSSR-Vol.-4-Iss.-1.pdf>, 128.

²³ Pereira, "IS's Social Media and Recruitment," 133.

²⁴ Brafman and Beckstrom, *Starfish and Spider*, 88, 89.

²⁵ Coleman, *Hacker Hoaxer, Whistleblower, Spy*, 293.

²⁶ Coleman, *Hacker, Hoaxer Whistleblower, Spy*, 302; Coleman writes how, "while my access to AntiSec grew, more activity seemed to be emanating from other, smaller hacker teams that I remained largely in the dark about."

²⁷ Brafman and Beckstrom, *Starfish and Spider*, 92.

²⁸ Coleman, “The Sabutage,” in *Hacker, Hoaxer, Whistleblower, Spy*; Coleman, *Hacker Hoaxer, Whistleblower, Spy*, 293.

²⁹ *Ibid.*

³⁰ Cronin, “How al-Qaeda Ends,” 13.

³¹ Arquilla and Ronfeldt, “Advent of Netwar,” 12.

³² Although the mission largely drives wolf pack attacks and lone wolf attacks, this same effect also inspires swarming attacks. However, since swarming attacks require greater coordination, they will materialize in a more traditional and deliberate way driven by leadership, not just a commitment to a broad mission.

³³ Mao Tse-Tung, “On Protracted War,” (speech, Yenan, China, May 26 to June 3, 1936), in *Selected Works of Mao Tse-Tung, Volume II*, accessed January 19, 2017, https://www.marxists.org/reference/archive/mao/selected-works/volume-2/mswv2_09.htm.

³⁴ Barack Obama, “Remarks by the President at the Cybersecurity and Consumer Protection Summit” (speech, Stanford, CA, February 13, 2015), Office of the Press Secretary, accessed January 14, 2017, <https://www.whitehouse.gov/the-press-office/2015/02/13/remarks-president-cybersecurity-and-consumer-protection-summit>.

³⁵ Coleman, *Hacker, Hoaxer, Whistleblower, Spy*, 379.

³⁶ *Ibid.*

³⁷ Coleman, *Hacker, Hoaxer, Whistleblower, Spy*, 215.

³⁸ *Ibid.*

³⁹ *Ibid.*

⁴⁰ *Ibid.*

⁴¹ Pereira, “IS Social Media and Recruitment,” 127.