P | I | P | S

The Cyber Collective Threat
A Pack of Lone Wolf Terrorists

PIPS White Paper 9.6: *Executive Summary*

Max Sterling, Research Fellow
Sarah Harmon, Research Intern

The cyber world enables the cyber collective, a robust and decentralized structure that lacks a strict chain of command and deliberate planning. 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 yet to be fully realized by a terrorist organization, but the actions of the Islamic State and Anonymous reflect the dangerous potential of this organizational structure.

Traditional Organizational Structures: Hierarchies and Networks

- *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. The hierarchy appeals to local groups that aspire to hold and govern territory. Although the hierarchy enables coordinated operations and territorial control, this structure remains exposed to leadership targeting.

- *Decentralized Networks*. The cells within a network exist as dispersed nodes whose members share a set of ideas and interests. The decentralized nature of a network enhances resilience and allows for a more global reach than a hierarchy, but the network less effectively governs and holds territory. Networks also dampen the impact of targeting operations. Subordinates have a greater degree of autonomy and flexibility, which makes networks harder to predict and preempt than hierarchies. Networks tend to be transnational and linked to religious or social ideology, which blurs the line between legitimate and illegitimate action.

The Cyber Collective Structure

The cyber collective is distinct from the network and hierarchy in three ways: (1) open membership instead of deliberate recruitment, (2) communication between circles and action spurred by catalysts, and (3) low coordination attacks driven by autonomous action (see Table 1).

- *Open Membership*. The cyber collective has a riskier recruitment process than traditional organizational structures. Members join of their own accord and most people use pseudonyms or remain anonymous online. The absence of a deliberate organizational plan creates diversity of membership, strategy, experience, and ambition, which makes the collective unpredictable and difficult to disrupt. Observing recruitment patterns becomes less effective, and the open-door membership policy increases the likelihood that a truly innovative, inspirational leader will join the organization.

- *Circles and Catalysts, not Cells and Commanders.* The cyber collective's circles and catalysts encourage a flexible organization and contribute to resilience. Catalysts wield their influence to create a circle or inspire action, but these leaders do not hold permanent power. Circles within the collective overlap, compete, and coordinate to conduct operations, so that no single leader or circle is critical to the overall operations.

- *Low-Coordination Attacks.* The three characteristic attacks of the cyber collective are unpredictable and nearly undetectable operations. Lone wolves will be most difficult to discover and disrupt and the least risk-averse. Wolf pack attacks conducted by a single circle will be similarly difficult to detect and can capitalize on the entire membership of the circle. Swarming attacks that require coordination between circles will be easiest to reveal, but benefit from greater numbers.

Implications for Counterterrorism

The nature of the cyber collective—its recruitment, structure, and attacks—produce challenges for counterterrorism efforts.

- *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. Moreover, should counterterrorism strategies dismantle a circle, the remnants could form new circles. Targeting a catalyst, a leader with temporary influence, would have a limited impact on the organization on the whole.

- *Problem of Detecting Attacks*. Bolstering defenses, detecting an impending attack, or preempting an operation will be problematic, both as a result of covert and quick online communication. Decentralized operations and open membership will produce inventive and daring operations, and attacks can be planned and executed hastily with limited risk consideration. Fractures between different circles produce competition, which leads to increasingly ambitious attacks.

- *Challenges of jurisdiction and distinguishability*. The cyber world complicates the process of determining legitimate versus illegitimate action. What constitutes an attack and what defines a combatant? Similarly, deciding which internal agency, country, or international organization should lead the fight will be difficult, and jurisdiction issues could slow the process of countering the organization.

Capacity in which Cyber Collectives Arise

Terrorist organizations can employ the cyber collective structure at different points during their lifespan according to their capabilities, goals, and standing. For instance, an organization without aspirations to become a traditional organization, like Anonymous, could exist solely in the form of a pure 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. An organization weakened by counterterrorism efforts, perhaps like the Islamic State, could be forced into the cyber collective structure. Lastly, a strong terrorist organization could broaden its reach and build a strong foundation for the future by developing a cyber collective.

Strategies to Fight the Cyber Collective

- *Challenge the Message*. The mission-driven nature of the cyber collective creates a dependence on messaging and communicating, both to draw in new members and to inspire action after the organization has formed. Fighting the message of the cyber collective can prevent autonomous attacks before they occur and initially dissuade people from joining the organization.

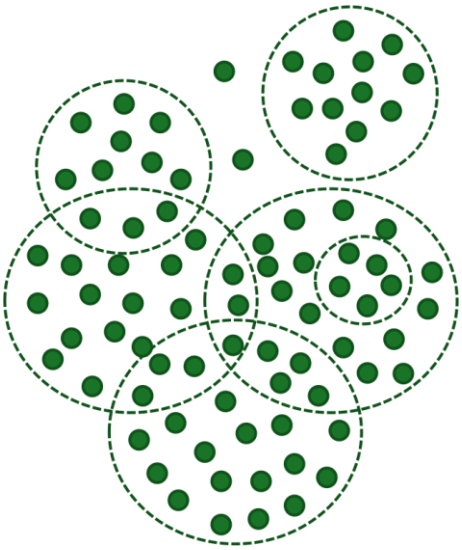
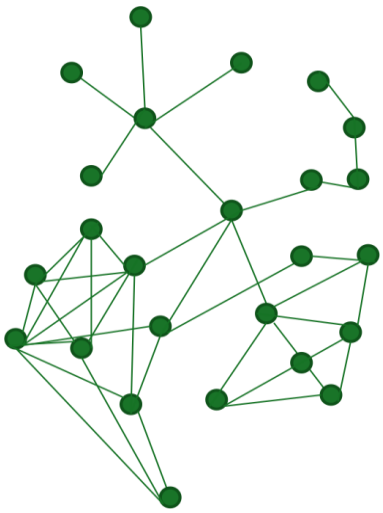
- *Disrupt the Recruitment Process.* Flooding the organization with fake members can force the organization to begin vetting earlier in the process. Stringent vetting will limit the diversity of the organization and slow operations. As members must prove or define their role and worth within the organization, the cyber collective will look more like a hierarchy or a network and can be targeted more easily.

- *Slow Operations.* 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 slow the operational pace. The cyber collective's most dangerous attacks are bold and come with little warning; operations that take more time to be realized will be more predictable, less threatening, and more likely to be detected and preempted.

Conclusion

The cyber world enables the emergence of a resilient, unpredictable terrorist threat: the cyber collective. Future strategies could exploit some key vulnerabilities of the cyber collective in efforts to challenge the organization's message, disrupt its recruiting process, and slow its operations. However, as terrorist groups learn more about how the cyber world can be used to enhance their organizations, the threat of a cyber collective grows. Examining this threat now will prevent tactical surprises from these dangerous terrorist organizations in the future.

Table 1: The Cyber Collective, Network, and Hierarchy

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