MITRE

SERIES
Number 20

INTELLIGENCE AFTER NEXT

USING INTENT-BASED INDICATIONS AND WARNING TO PREVENT TERRORIST CYBER ATTACKS

by Dan Kolva, Chris Ante, Taye Folk

Cyber: The Next Evolution of Terrorism Tactics

Significant terrorist attacks via the cyber domain could be the next evolution in terror tactics. For a very long time, foreign terrorist organizations (FTOs) have used terrorism tactics to achieve political end states. While the United States, partners, and allies have countered terrorist organizations quite visibly over the past two decades, FTO threats still linger. Terrorist organizations have lost ground in the physical space, but their online presence continues. FTOs make significant efforts to recruit, equip, plan, and coordinate attacks and spread their ideology online.*

As the availability of cyber threat tools increases and the capability of cyber threat actors becomes easier to develop, our strategies should also change to counter this potential threat. According to a recent RAND research report, "Terrorist groups, whether centralized or decentralized, might have access to advanced means to facilitate attacks: increasingly affordable and available Unmanned Aerial Systems (UASs); data networking, artificial intelligence, and cyber know-how; and, possibly, biological agents."[1] We need to plan and prepare now to get ahead of these advanced means for terror attacks. Forewarning of terrorism threats via the cyber domain will be crucial.

The 2018 National Strategy for Counterterrorism (CT) of the United States includes the cyber domain as an area requiring protection from terrorism. To counter terrorist ideologies, the CT strategy of 2018 intended to "combat terrorist use of cyberspace as a global stage to showcase their violent ideologies, to fundraise, and to radicalize, recruit, and mobilize individuals to violence."[2] However, these actions are focused on terrorist content and not terrorist computer network operations or attacks. Additionally, the strategy fails to mention proactive measures to be taken to develop cyber-based indications and warning before a terrorist-conducted event occurs.

The 2023 National Cybersecurity Strategy calls for countering financing of terrorism via ransomware, the use of illicit cryptocurrency, and supporting efforts to eliminate terrorist content online.[3] Unfortunately, these actions do not address indications and warning (I&W) of terrorist actors with terrorist intent and will likely not address the threat before an attack, when it would most reduce the effectiveness of a terrorist cyber attack.

IT MAY BE ONLY A MATTER OF TIME BEFORE TERRORIST ORGANIZATIONS DECIDE TO LEVERAGE MALICIOUS MALWARE AND SERVICES TO CONDUCT ATTACKS AGAINST U.S. CRITICAL INFRASTRUCUTRE OR OTHER ELEMENTS OF SOCIETY HEAVILY DEPENDENT ON THE INTERNET

Countering terrorist tactics of the past was predominately based on territory. The next evolution of terrorism tactics likely will include more cyber-based threats; we should consider a pivot in both counterterrorism and cybersecurity to counter terrorist cyber-based threats. Enhancing early warning of potential cyber threats from foreign terrorists should be considered. This would mean *including a cyber component in the National Counterterrorism Strategy as well as including specific terrorism threats in the National Cyber Strategy while implementing both strategies*.

Overall, we need to consider developing I&W geared more toward cyber threat actor intent. Contrary to popular thought within the cybersecurity field, intent matters. An understanding of intent can alter how an incident is handled. Threat actors with intent on destruction, harm to the population, and/or evoking a degradation of trust in government could have an outsized effect. There may be no tactical difference in how a terrorist cyber attack is conducted. Therefore, we need to further develop the specific indicators that would distinguish terrorist cyber-threat actors from criminal actors and plan for the appropriate and likely different response to terrorists.

*For the purposes of this paper, foreign terrorist organizations are the primary concern. Domestic terrorism threats can certainly develop the same cyber attack capability. The domestic terrorism threats via the cyber domain deserve similar consideration in a separate paper or discussion.

The Current Environment for Threat Actors in the Cyber Domain

Malicious cyber tools and services are increasingly more available and have been used across the spectrum of threat actors, ranging from state-sponsored adversaries to cybercriminal organizations to affiliates of Ransomware-as-a-Service (RaaS) programs.[4] These cyber threat actors choose to use these tools not only because of their accessibility, but also because they very efficiently carry out their objectives. The wealth of available malicious cyber tools and services allows an adversary to pick and choose from a variety of options that can be obtained through publicly available forums and through sources such as marketplaces on the dark web.

Ransomware is a prime example of a capability that has become easy to both obtain and use against selected targets by criminal actors for financial gain. Conti ransomware is a specific strain of ransomware that has caused major disruptions. Conti is a prolific RaaS that has impacted various healthcare entities, including a hospital in New Mexico in February 2021 and the Irish national healthcare system in May 2021.[5] In August 2021, one of the affiliates of Conti's RaaS program leaked playbooks containing details about operating on compromised victim networks.[6] The level of detail in these playbooks was comprehensive enough to inform individuals on how to carry out full ransomware operations, specifically for Conti. The accessibility and availability of cyber resources now allow any interested party, including terrorists, to employ malicious cyber tools, cause significant disruption, and instill fear, panic, and chaos.

Scenario: FTO Conducts a Cyber Attack Like Colonial Pipeline

A successful terrorist cyber attack combined with an effective messaging campaign could have detrimental effects on the greater population. The ransomware attack on Colonial Pipeline in May 2021 captured headlines around the world showing panicked Americans buying up much of the available fuel supply and causing shortages. Vulnerabilities of our connected infrastructure came to light.[7] What if the Colonial Pipeline cyber attack[8] [9] was conducted by a foreign terrorist organization intending to cause that fear, panic, and chaos? The difference between cyber attacks with criminal intent (i.e., financial gain) and cyber attacks with terrorist intent (i.e., causing fear, panic, and chaos for political gain) may only be a few keystrokes, if any at all. The result could be the difference between short-term annoyance versus harm to national security.

A terrorist cyber attack has the potential to have an outsized effect and significant consequence largely because of the perceived fear factor a terrorist organization may bring. We observed only a glimpse of this with the Colonial Pipelines cyber attack, in which the cyber threat actors had only criminal intent. The pipeline was shut down for precautionary reasons, and the ransomware did not directly impact the industrial control system. However, significant damage occurred due to public fear of losing access to the fuel supplied by the pipeline. This happened without a significant messaging campaign to the public. A cyber attack like this, combined with an FTO claiming responsibility via a messaging campaign, as we often see in terrorist attacks, could significantly increase the fear, panic, and chaos following the attack.

The Future Environment for Threat Actors in the Cyber Domain: Hybrid Threats

The numerous threats to the U.S. tend to overlap, to include cyber threats, terrorism threats, and threats from great power competition; thus there is a need to ensure our countering strategies have the right amount of overlap. An example of all three threat elements overlapping is the Russian Private Military Company (PMC) Wagner, recently designated a Transnational Criminal Organization (TCO) due to war crimes it has committed in Ukraine and other documented crimes throughout the Middle East and Africa.[10] [11] [12] PMC

Wagner is active in the cyber domain, conducting influence operations in Africa, fueling terrorism, and often exploiting anti-Western sentiment.[13] [14] In early March 2023, U.S. Attorney General Merrick Garland said he would "not object" to labeling Wagner as an FTO, and referred to Yevgeny Prigozhin, the owner of PMC Wagner, as a "war criminal."[15] It is very possible for hybrid threats like PMC Wagner and other FTOs to use malicious cyber tools and services available for cyber attacks, possibly in conjunction with physical attacks designed to further erode public trust in government institutions. Attacks like these would pose threats to U.S. persons, U.S. facilities, and other interests overseas.

A TERRORIST CYBER ATTACK HAS THE POTENTIAL TO HAVE AN OUTSIZED EFFECT AND SIGNIFICANT CONSEQUENCE LARGELY BECAUSE OF THE PERCEIVED FEAR FACTOR A TERRORIST ORGANIZATION MAY BRING

Combined Strategic Effort: Enhance Counterterrorism and Cybersecurity

We should implement both the new counterterrorism strategy and the new cybersecurity strategy by ensuring they both include elements to identify and defend against FTOs that may intend to conduct significant attacks via the cyber domain. The first recommendations below are to enhance the counterterrorism and cybersecurity strategies directly. The remaining recommendations relate to enhancing current efforts with both CT and cybersecurity in mind.

- **Enhance our counterterrorism strategy.** Since the publication of the 2018 CT strategy, a new U.S. counterterrorism strategy and the implementing plan is underway. The new counterterrorism strategy has not yet been publicly released but, according to a recent New York Times article citing sources at the National Security Council, "The strategy is said to respond to how the terrorist threat has evolved over time — it is more diffuse, ideologically diverse, and geographically dispersed — and the need for the United States to prioritize threats amid competing problems and resource constraints, including those involving Russia, China, cybersecurity, climate change and the coronavirus pandemic. The strategy is also said to emphasize other means of reducing the risk of terrorism, including working with partner forces, and supporting overseas civilian law enforcement abilities, while reserving U.S. kinetic action as a tool where merited."[16] While implementing this new strategy, we should consider further development of I&W for FTOs to conduct attacks via the cyber domain.
- **Enhance our cybersecurity strategy.** While implementing the new cybersecurity strategy, we should ensure we build in I&W specific to terrorist use of ransomware, illicit cryptocurrency, and content platforms. This would help network defenders and decision makers alike prioritize threats in a way that looks at the threat more holistically and includes the potential effect of a successful attack. While an FTO cyber threat event may be considered unlikely, it could still have a high-impact or outsized effect, as mentioned earlier. Additionally, developing specific FTO-oriented I&W could go a long way in preventing these high-impact cyber attacks.
- **Work with foreign partners.** Geographic areas currently developing communications infrastructure, including regions in Africa, may be particularly at risk for cyber threats. Africa is one of the fastest growing regions when it comes to internet penetration.[17] This new and rapidly developing digital infrastructure is exploited by cyber criminals and is one of the most pressing challenges plaguing economic activity in Africa.[18] This digital environment has the potential to be exploited by FTOs as well. Working with partners, particularly in areas where groups like PMC Wagner are active in the cyber domain, could help align U.S. partners with the cybersecurity initiatives developed to better secure the U.S. critical infrastructure.[19] The U.S. State Department

is currently working with Congress to develop formal cyber aid programs that could help partners with suitable concepts, organizational structures, cyber best practices, and templates that could assist in regulating these rapidly developing digital infrastructures.[20]

- **Support overseas civilian law enforcement.** The U.S. Department of Justice, with specific programs like the International Computer Hacking and Intellectual Property (ICHIP) Network, has numerous law enforcement partnerships overseas.[21] Building partner capacity to develop effective cybercrime laws, as well as developing the capability to enforce and prosecute those laws, will help enhance U.S. national security from cyber threats overseas, including threats from FTOs active in the cyber domain. Developing more ICHIP offices and similar efforts overseas should be considered when implementing the new counterterrorism and cybersecurity strategies.
- **Develop indications and warning for FTO significant attacks via the cyber domain.** The information in this area pales in comparison to our understanding of state-sponsored and cybercriminal activities. This may be due to a lack of visibility into FTO cyber activities or a lack of FTO-conducted cyber activity overall. However, this should not preclude network defenders, intelligence analysts, or policymakers from being proactive with counterterrorism in cyberspace. Open-source intelligence around FTO-based cyber activities is extremely limited, though there are a few public sources referencing this activity. In 2021, the cybersecurity firm Clearsky linked a campaign of malicious cyber activity to Hezbollah, which the U.S. Department of State has designated as an FTO.[22] This activity included the hacking of web servers across the U.S., United Kingdom, and Middle East, but did not cause any substantial damage. The Islamic State (ISIS) has also been noted to have the potential to deploy cyber capabilities, if they so choose.[23]
- **Better align building partner capacity for counterterrorism and cybersecurity.** In addition to long-established building partner capacity (BPC) programs in counterterrorism, the U.S. should align BPC efforts to counter threat actors operating via the cyber domain. In effect, counterterrorism and cybersecurity capacity building could work together. This would be particularly useful in countries developing new communications infrastructure (with assistance from great power competitors), where many partner nations could be at risk for cyber threats. Building capacity in both counterterrorism and cybersecurity should include the development of policies, laws, and law enforcement capabilities to effectively counter online threats.

WE SHOULD IMPLEMENT BOTH THE NEW COUNTERTERRORISM STRATEGY AND THE NEW CYBERSECURITY STRATEGY BY ENSURING THEY BOTH INCLUDE ELEMENTS TO IDENTIFY AND DEFEND AGAINST FOREIGN TERRORIST ORGANIZATIONS THAT MAY INTEND TO CONDUCT SIGNIFICANT ATTACKS VIA THE CYBER DOMAIN

We need well-coordinated CT and cybersecurity strategies from both government and industry sectors. Industry would be focused on I&W, while government would assist via education, coordination, and working with foreign partners to ensure that laws are present and enforceable. Altogether, counterterrorism and cybersecurity efforts should be set up for success with strategies that prevent terrorist attacks via the cyber domain.

Let's Get After It!

The best time to deal with a devastating terrorist attack is before it happens. Foreign terrorist organizations and the cyber threat actors who may support them

will likely adapt and use the ever-growing number of tools available in the cyber domain to conduct attacks that could physically harm U.S. citizens. Implementing counterterrorism and cybersecurity strategies should help prevent terrorists from causing fear, panic, and chaos via the cyber domain.

Additional analysis and planning are required to prepare the U.S. for terrorist cyber threat actors utilizing malicious cyber tools and services for the purposes of terrorism. We must first ensure that we understand the indications and warning associated with an FTO significant attack via the cyber domain. Then we must ensure we have the required tools in place to prevent terrorist cyber attacks before they occur and have a tailored response when they do.

Endnotes

1. Terrence K. Kelly, David C. Gompert, and Karen MSudkamp, "Terrorism Net Assessment," RAND Corporation, 2023.

2. White House, "National Strategy for Counterterrorism of the United States of America," October 2018.

3. White House, "National Cybersecurity Strategy," March 2023.

4. Microsoft, "Ransomware As A Service: Understanding The Cybercrime Gig Economy and How to Protect Yourself," May 9, 2022.

5. U.S. Department of Health and Human Services, "Conti Ransomware and the Health Sector," July 8, 2021.

6. Recorded Future, "Disgruntled Ransomware Affiliate Leaks The Conti Gang's Technical Manuals," August 5, 2021.

7. Easterly, Jen,"The Attack on Colonial Pipeline: What We've Learned & What We've Done Over the Past Two Years," CISA Director, May 7, 2023.

8. Krebs on Security, "A Closer Look at the DarkSide Ransomware Gang," May 11 2021.

9. Bloomberg, U.S. Edition, "Colonial Pipeline Paid Hackers Nearly $5 Million in Ransom," May 13, 2021.

10. Treasury Department, "Treasury Sanctions Russian Proxy Wagner Group as a Transnational Criminal Organization," January 2023.

11. The Hill, "Designating Wagner Group as a Transnational Criminal Organization is a First Step — But There's More Work To Do," February 2, 2023.

12. James Petrila and Phil Wasielewski, "It's Time to Designate Wagner Group as a Foreign Terrorist Organization," Lawfare, June 30, 2022.

13. Clarke, Colin, "How Russia's Wagner Group is Fueling Terrorism in Africa," Foreign Policy, January 25, 2023.

14. Walsh, Declan, "Putin's Shadow Soldiers: How the Wagner Group Is Expanding in Africa," New York Times, May 31, 2022.

15. Colin Clarke, Christopher Faulkner, Raphael Parens, and Kendal Wolf, "The Wagner Group's Expanding Global Footprint," Foreign Policy Research Institute, Eurasia Program, April 2023.

16. Savage, Charlie, "White House Tightens Rules on Counterterrorism Drone Strikes," New York Times, October 7, 2022.

17. Cyber Security Africa Summit, website for Cyber Security Africa Summit 2022, accessed on November 17, 2022.

18. Cyber Security Africa Summit, website for Cyber Security Africa Summit 2022, accessed on November 17, 2022.

19. White House, "National Security Memorandum on Improving Cybersecurity for Critical Infrastructure Control Systems," July 28, 2021.

20. Matishak, Martin, "State Department, Congress Working on Formal Program For U.S. Cyber Aid," Recorded Future, April 12, 2023.

21. Department of Justice, official website for the U.S. Department of Justice, accessed on November 17, 2022.

22. ZDNET, "Hezbollah's Cyber Unit Hacked Into Telecoms And ISPs," January 28, 2021.

23. National Public Radio, "ISIS Uses Cyber Capabilities to Attack the U.S. Online," April 25, 2016.

Authors

Dan Kolva is a Group Leader at MITRE with expertise in strategic intelligence, strategic planning, and counterterrorism. He transitioned to his current role following a 21-year career in the U.S. Army as an Air Defense Artillery and Strategic Intelligence Officer. Dan has a B.S. from the University of South Carolina, an M.S. from the National Intelligence University, and a Graduate Certificate in Cyber Threat Intelligence from James Madison University.

Chris Ante is a Senior Cyber Security Engineer and Group Leader at MITRE focusing on cyber threat intelligence and emerging technologies. He previously worked as a Technology Consultant for IBM and as the Program Director of Cybersecurity for the National Student Leadership Conference. Chris has a B.S. in Business Information Technology from Virginia Tech.

Taye Folk is an Intermediate Systems Engineer at MITRE interested in technology and social sciences. Through her undergraduate research and experience, Taye has supported the Fairfax County Fire and Rescue Department. She has a B.S. in Criminology, Law and Society from George Mason University and is currently pursuing a M.S. at George Mason University.

Intelligence After Next

MITRE strives to stimulate thought, dialogue, and action for national security leaders developing the plans, policy, and programs to guide the nation. This series of original papers is focused on the issues, policies, capabilities, and concerns of the Intelligence Community's workforce as it prepares for the future. Our intent is to share our unique insights and perspectives surrounding a significant national security concern, a persistent or emerging threat, or to detail the integrated solutions and enabling technologies needed to ensure the success of the Intelligence Community. The views expressed in this publication are those of the author(s) and do not imply endorsement by the Office of the Director of National Intelligence or any other U.S. government department/agency.

About MITRE

MITRE's mission-driven teams are dedicated to solving problems for a safer world. Through our public-private partnerships and federally funded research and development centers, we work across government and in partnership with industry to tackle challenges to the safety, stability, and well-being of our nation.

MITRE

AUGUST 2023