Technology and the Crime-Terror Nexus: Threat Convergence in a Digital Age

Steven Inglis

Abstract

Over the past three decades, scholars and national security authorities have devoted increasing attention to threats involving the so-called "crime-terror nexus," which describes varying levels of interaction and overlap between criminal and terrorist entities. Despite widespread acknowledgement that information technology has played a significant role in expanding the crime-terror nexus, details of this phenomenon remain unexplored. To fill this gap, this article explores how communications technology, and the Internet in particular, impacts the crime-terror nexus by opening additional pathways for interaction and acquisition of novel resources and capabilities among criminal and terrorist organizations. To that end, it presents both objective evidence of crime-terror cooperation and hybridization in cyberspace, as well as analysis of likely current and future uses of the Internet that may be impacting the nexus. This article concludes with policy recommendations that security authorities should consider among efforts to address the risks associated with technology and the crime-terror nexus.

The views expressed herein are those of the author alone and do not reflect the views of the U.S. Government or any other organization with which the author has been associated, past or present.

Introduction

In July 2007, a U.K. court found al-Qaida's "god-father of cyberterrorism" and two co-defendants guilty of using the Internet to incite murder through terrorism.[1] Younis Tsouli and his accomplices employed computer viruses and phishing scams to steal 37,000 credit card numbers, which in turn financed online bomb-making tutorials, videos of beheadings, and operational resources for proposed terrorist attacks in the United States, Europe, and the Middle East.[2] This anecdote demonstrates how criminal means can be employed for terrorist ends, and is indicative of an emerging relationship between crime and terrorism that has been observed in academic and government circles in recent decades.

The "crime-terror nexus," as this phenomenon has come to be called, refers to overlapping criminal and terrorist activities, both through cooperation in quid pro quo arrangements and through hybridization, wherein terrorists adopt the methods of criminals to further their goals, or vice versa. Although these phenomena have been well documented in existing academic literature, the above example lends credence to the existing notion that technology is playing a significant role in widening the crime-terror nexus.

This article is intended to fill a significant void in research on this topic by presenting the first in-depth look at how technology, and information technology in particular, is "blurring the lines" between crime and terrorism. The article begins with a conceptual definition of the crime-terror nexus, followed by a literature review that demonstrates the extent of the threat and the need for additional research on this subject. It then analyzes both real and theoretical manners in which cyberspace enables cooperation between criminal and terrorist actors and the hybridization of terrorist and criminal groups. After assessing the likely implications for U.S. national and transnational security, the article sets forth several policy recommendations that decision makers may consider to mitigate the risks posed by this threat. The findings herein confirm suspicions posed in previous research—that technology plays a significant role in widening the crime-terror nexus—but also suggest that cyberspace is a major and under-acknowledged environment in which criminals and terrorists can exchange goods and services, learn from one another, and employ the "other's" methods to accomplish their malicious objectives.

Defining the Crime-Terror Nexus

Scholars have traditionally distinguished criminals from terrorists by contrasting their

[1] See Mark Oliver, "'Internet jihadist' jailed for 10 years," *The Guardian,* 5 July 2007, http://www.theguardian.com/technology/2007/jul/05/terrorism.uknews; Brian Krebs, "Three Worked the Web to Help Terrorists," *The Washington Post*, 6 July 2007, http://www.washingtonpost.com/wpdyn/content/article/2007/07/05/AR2007070501945.html.

[2] Ibid.

motives. Criminals are said to be driven primarily by the prospect of economic gain, while terrorists seek to realize some political or ideological ideal.[3] Notwithstanding these delineations, scholars posit that criminal and terrorist organizations have each changed considerably as a result of post-Cold War trends, including the spread of diaspora communities around the globe, the rise of weak and failed states, a decrease in state sponsorship of terrorism, and the growing interconnectedness of global financial markets.[4] This evolution has affected both the methods and motives that each categorical group employs to further its goals, and is blurring the lines that have previously distinguished crime from terror.[5] The crime-terror nexus represents a conceptual framework that attempts to describe these dynamic phenomena. Accordingly, it is an umbrella term used to describe several degrees and directions of interplay between crime and terror, individual criminals and terrorists, and criminal organizations and terrorist groups.

Based on an extensive review of existing academic literature and accounting for the wide array of activities that the nexus represents, the crime-terror nexus can be said to comprise two component phenomena: *crime-terror cooperation* and *crime-terror hybridization*. Crime-terror cooperation occurs when criminals and terrorists interact for mutual gain, and involves the quid pro quo exchange of money, goods, services, or knowledge. It includes one-time transactions, as when Mansour Arbabsiar, a member of the Iranian Revolutionary Guard Corps, attempted in 2011 to pay $1.5 million to hire a purported member of the Los Zetas drug cartel to assassinate the Saudi Arabian Ambassador to the United States.[6] Yet cooperation involving certain activities may also become routine and habitual. The Department of Justice reported in 2010 that 29 of the 63 organizations on its Consolidated Priority Organization Targets (CPOT) list, which designates drug trafficking organizations (DTOs) that threaten the United States, were associated with terrorist groups.[7]

Crime-terror hybridization describes a nexus between terrorist and criminal activities, but not necessarily between organizations. Hybridization occurs when a terrorist network undertakes criminal acts and schemes to further its goals; both al Qaeda and the Islamic State, for example, are said to have acquired significant wealth from direct participation in the lucrative Afghan heroin trade.[8] Hybridization also occurs when a criminal organization engages in terrorist-style attacks to

[3] See, for example, Jack Jarmon, *The New Era in U.S. National Security: An Introduction to Emerging Threats and Challenges*, (Lanham, MD: Rowman & Littlefield, 2014), 166.

[4] Tamara Makarenko, "The Crime-Terror Continuum: Tracing the Interplay between Transnational Organised Crime and Terrorism," *Global Crime* 6:1 (February 2004): 130, doi: 10.1080/1744057042000297025.

[5] Ibid., 130-131.

[6] U.S. Department of Justice, "Two Men Charged in Alleged Plot to Assassinate Saudi Arabian Ambassador to the United States," October 11, 2011, https://www.justice.gov/opa/pr/two-men-charged-alleged-plot-assassinate-saudi-arabian-ambassador-united-states.

[7] The White House, National Security Council, "Transnational Organized Crime: A Growing Threat to U.S. National and International Security," accessed April 14, 2015, https://obamawhitehouse.archives.gov/administration/eop/nsc/transnational-crime/threat.

[8] "High finance: ISIS generates up to $1bn annually from trafficking Afghan heroin," *Russia Today,* 6 March 2015, http://rt.com/news/238369-isis-drug-money-trafficking/

incite public fear, create public doubt in government institutions, or weaken a local regime.[9] Historical examples include the Medellin Drug Cartel's 1989 bombing of Avianca Flight 203, which was intended to derail forthcoming presidential elections.[10]

The crime-terror nexus, therefore, describes several convergent activities and connects a wide array of nefarious actors, all toward ends that involve the exploitation of tenuous security environments to their benefit. The nexus has, by its nature, expanded to serve both transnational organized crime and terrorism, and therefore broadens the power, scope, and influence of both traditional categorical groups.

Literature Review

The United States law enforcement and intelligence communities, as well as international security bodies, have publicly acknowledged the threats posed by the crime-terror nexus. In 2010, for the first time, the U.S. National Security Strategy characterized the crime-terror nexus as a "serious concern as terrorists use criminal networks for logistical support and funding."[11] Former Director of National Intelligence James Clapper stated in a January 2012 congressional hearing that transnational organized crime and its connections with international terrorism were among the nation's "most pressing national security concerns."[12] Department of Defense officials told the Senate in March 2012 that "the two missions of fighting terrorism and combating global organized crime are increasingly linked."[13] In April 2015, U.N. Secretary General Ban Ki-moon observed that, "Like never before, terrorists and criminals around the world are coming together and feeding off each other."[14] In short, U.S. and international policy circles have acknowledged the emergence of the crime-terror nexus and have incorporated the term into the lexicon of international security. While academics have conducted substantial research on the relationship between crime and terrorism, most simply acknowledge the importance of technology in the emergence of the crime-terror nexus without adding further analysis. Hesterman (2004) notes that technology and globalization are primary factors that contribute to the growth of transnational crime and further terrorist agendas.[15] Makarenko (2004) states that organized crime and terrorism have taken

[9] Tamara Makarenko, "Foundations and evolution of the crime-terror nexus," in *Routledge Handbook of Transnational Organized Crime*, eds. Felia Allum and Stan Gilmour (New York: Routledge, 2012), 236.

[10] Paula Carrillo, "Twenty-five years on, Colombia mourns Escobar plane bombing," *Yahoo! News*, 28 November 2014, https://sg.news.yahoo.com/twenty-five-years-colombia-mourns-escobar-plane-bombing-231712149.html.

[11] The White House, "National Security Strategy," May 2010, https://www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf.

[12] John Rollins and Liana Sun Wyler, *Terrorism and Transnational Crime: Foreign Policy Issues for Congress* (CRS Report No. R41004) (Washington, DC: Congressional Research Service, 2013), 2, http://fas.org/sgp/crs/terror/R41004.pdf.

[13] Karen Parrish, "Link Grows Between Terrorism, Organized Crime, Officials Say," *DoD News*, March 28, 2012, http://www.defense.gov/news/newsarticle.aspx?id=67721.

[14] "UN chief says 'crime and terrorism' feed off each other," *Al Jazeera,* 12 April 2015, https://uk.news.yahoo.com/un-chief-says-crime-terrorism-feed-off-other-164510934.html#GHfE0DN.

[15] Jennifer L. Hesterman, "Transnational Crime and the Criminal-Terrorist Nexus: Synergies and Corporate Trends," (Research Report, Air University, 2004), 59, http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA424418.

advantage of post-Cold War access to technological advancements, which have blurred the lines between politically and criminally motivated violence.[16] Wang (2010) cautions that the crime-terror nexus could leverage communications technology and advanced equipment to evade law enforcement and intelligence.[17] Forest (2012) warns of the "vast unregulated space of the Internet, where various kinds of crime-terror collaboration can be facilitated."[18] The Congressional Research Service (2013) calls cyberspace one of the "key nodes" where crime-terror interaction is most likely to occur.[19] Unfortunately, while these scholars unanimously draw attention to the role of technology in enabling the crime-terror nexus, they do not explain in greater detail how technology interacts with the nexus.

Only two analyses broach the impact of technology on crime and terror generally, but neither explicitly addresses crime-terror interactions. Shelley (2003) examines a thematic overview of how criminals and terrorists use cyberspace, and Holt (2012) outlines how the Internet and computer-mediated communications affect crime, terrorism, and the definitions thereof. Beyond these studies, there has been no specific academic research into how information technology expands the crime-terror nexus, making this topic ripe for academic inquiry.

Trends in Technology Impacting Crime and Terrorism

The information revolution has introduced trends in the use of technology that impact the way organized criminals and terrorists operate. The expansion of air travel in the late 20th century, along with the globalization of business, have made it easier for terrorists and organized criminals to move goods, money, and people across borders.[20] Enhanced, anonymous communications capabilities via cell phone and the Internet further facilitate the coordination of malicious activities. Shelley and Picarelli argue that chief among commonalities between terrorists and transnational criminals is their regular use of information technology to plan and execute operations.[21] Logically then, interaction between the two sets of actors becomes more likely as technology shrinks the time and space required to communicate and exchange ideas, goods, and services.

The potential for increased crime-terror interaction is especially augmented in cyberspace, where the ease of communication and number of targets available to both criminals and terrorists is expanding dramatically. Given the rapid rate at which people and devices are connecting to the Internet in the 21st century, the potential vulnerabilities inherent to information technology (IT) risk, defined as the associated risks that come with tying any resource to some type of information

[16] Makarenko, 130.

[17] Wang, 15.

[18] James J.F. Forest, "Crime-Terror Interactions and Threat Convergence," Comments prepared for TransAtlantic Dialogue on Combating Crime-Terror Pipelines (June 2012), 5, http://www.jamesforest.com/wp-content/uploads/2012/06/JForest-CrimeTerror_Dialogue_June2012.pdf.

[19] Rollins and Wyler, 1.

[20] Steven D'Alfonso," Why Organized Crime and Terror Groups Are Converging," *Security Intelligence*, 4 September 2014, http://securityintelligence.com/why-organized-crime-and-terror-groups-are-converging/#.VTKO8tJVhBc.

[21] Louise I. Shelley, "Organized Crime, Terrorism, and Cybercrime," in *Security Sector Reform: Institutions, Society, and Good Governance,* eds. Alan Bryden and Philipp Fluri (Baden-Baden: Nomos, 2003), 303, http://www.crime-research.org/library/ Terrorism_Cybercrime.pdf.

technology (i.e. a database, bank account, or personally identifiable information), are multiplying, perhaps at an exponential rate. Intel co-founder Gordon Moore famously predicted in 1965 what came to be known as Moore's Law—the idea that computer speed per unit cost would rise exponentially over time.[22] Moore's Law has since been applied to describe technological change more broadly, and its implications for security are immense.[23] In this sense, the proliferation of new technologies will significantly increase the number of security vulnerabilities that permit nefarious actors to attack individuals, organizations, and nation-states.

These developments yield new challenges for law enforcement and intelligence authorities. As Stewart Baker, former NSA general counsel, claims, "Moore's Law is working more for the bad guys than the good guys […] It's really 'Moore's outlaws who are winning this fight."[24] Baker's assessment is correct in at least one manner, as the remaining sections of this article demonstrate—the enhanced ability to interact online, coupled with a dramatic rise in the number of targets available via the Internet to both criminals and terrorists, makes it logical to expect that each set of actors will more frequently use online environments to exchange knowledge and expertise as well as adopt one another's tactics to achieve their illicit goals.

Technology and Crime-Terror Cooperation

At least three prominent trends are enabling crime-terror cooperation in cyberspace: the rise of anonymity tools, the ease of information exchange, and the rise of crime-as-a-service (CaaS) and underground marketplaces in online environments.

Anonymity Tools

The emergence of online anonymity tools helps to remove preexisting disincentives for cooperation between criminals and terrorists, including distrust, competition, ideological resistance, and the higher likelihood of law enforcement detection that exists offline.[25] Within the so-called deep web, or the portion of the World Wide Web that is unindexed by standard search engines, are darknets including Tor ("The Onion Router") that provide almost complete anonymity in cyberspace. This technology was created with good intentions—to protect civil liberties, for example—but provides malicious actors with an alternative to potentially dangerous or suspect in-person interaction. The anonymity of cyberspace provides a more "comfortable" environment in which illicit deals can be struck, expertise can be exchanged, and services can be rendered without the dangers associated with real life contact. Of equal importance, senders and recipients of illicit goods and services may have no idea with whom they are interacting—a deep web arms dealer who

[22] Ray Kurzweil, "The Law of Accelerating Returns," Kurzweil Accelerating Intelligence, 7 March 2001, http://www.kurzweilai.net/the-law-of-accelerating-returns.
[23] Ibid.
[24] David Talbot, "Moore's Outlaws," *Technology Review,* 22 June 2010, http://www.technologyreview.com/featuredstory/419452/moores-outlaws/.
[25] Rollins and Wyler, 6.

would otherwise be ideologically opposed to supporting terrorism, for example, might be entirely unaware that a given buyer is a member of a Jihadi extremist group. This example, while hypothetical, seems likely given the acknowledged existence of arms dealers on the deep web.[26]

Exchange of Expertise

The exchange of technical know-how has been a prominent component of crime-terror cooperation in recent decades. In 2001, for example, U.S. and Colombian investigators discovered that the Revolutionary Armed Forces of Colombia (FARC), itself a hybrid crime-terror organization, paid $2 million to the Irish Republican Army to have members of its engineering department demonstrate techniques for bomb and mortar making.[27] Similar arrangements online are becoming more likely as the number of terrorist and criminal Internet users rises. Cybercrime expert Marc Goodman writes that in digital environments, illicit actors will "often learn from and imitate the operational success of one another."[28] Likewise, the FBI reports that terrorists are demonstrating an increased interest in cyberattacks.[29] Given that analysts have observed a gap between the cyberattack capabilities of terrorist groups and the hacker community at large, it follows that terrorists seeking to exploit cyber capabilities will turn to cyber criminals for online know-how.[30] Along those lines, Goodman claims that portions of the Internet are becoming something of a "criminal university," where terrorists can learn how to run a phishing scam, defeat firewalls, steal credit card data, and hack various devices.[31]

Crime-as-a-Service and Underground Marketplaces

Perhaps more ominous and impactful to the crime-terror nexus are burgeoning "Crime-as-a-Service" (CaaS) offerings and underground marketplaces that allow terrorists to easily purchase an array of criminal services, both online and offline. CaaS marketplaces offer a variety of products, including pay-per-install malware, money laundering services, anonymity tools, and botnets for rent.[32] Acknowledging this threat, the FBI observes that "botnets run by criminals could be used by cyberterrorists … to steal sensitive data, raise funds, limit attribution of cyberattacks, or disrupt access to critical national infrastructure."[33] Similarly, Assistant Attorney General John Carlin of the

[26] Thom Patterson, "Inside the illegal online weapons trade," *CNN*, 11 August 2016, http://www.cnn.com/2016/08/10/us/declassified-illegal-online-weapons-trade/.

[27] Jennifer L. Hesterman, *The Terrorist-Criminal Nexus: An Alliance of International Drug Cartels, Organized Crime, and Terror Groups,* (Boca Raton, FL: Taylor and Francis Group, 2013), 279.

[28] Marc Goodman, *Future Crimes* (New York: Doubleday, 2015), 25.

[29] Damian Paletta, "FBI Director Sees Increasing Terrorist Interest in Cyberattacks Against U.S." *Wall Street Journal,* 22 July 2015, http://www.wsj.com/articles/fbi-director-sees-increasing-terrorist-interest-in-cyberattacks-against-u-s-1437619297.

[30] Thomas J. Holt, "Exploring the Intersections of Technology, Crime, and Terror," *Terrorism and Political Violence* 24:2 (2012), 346, doi: 10.1080/09546553.2011.648350.

[31] Goodman, 187.

[32] Europol. *The Internet Organised Crime Threat Assessment (iOCTA) 2014*. The Hague: European Police Office, 2014.

[33] *Cybersecurity: Responding to the Threat of Cybercrime and Terrorism*, 112th Cong, statement of Gordon M. Snow,

U.S. Department of Justice's National Security Division reported in June 2016 that "blended threats" are emerging as criminals begin to offer their tools for a profit.[34]

Underground marketplaces in the deep web also offer goods and services that may facilitate offline crime and terror. Several of these services may be used to facilitate acts of terrorism and include the sale of counterfeit and fraudulently obtained identification documents, murder-for-hire, weapons and explosives, counterfeit currency, and human trafficking services.[35] Recent news reports suggest that ISIS and other designated terrorist organizations can buy U.K. passports on the deep web.[36] Furthermore, bitcoin and other cryptocurrencies facilitate clandestine dealings by enabling rapid purchases and, in comparison with traditional finance, relatively untraceable transactions.

Technology and Crime-Terror Hybridization

Evidence of the hybridization of transnational organized crime and terrorist groups also exists online. One of the most prevalent characteristics of technology's influence on the crime-terror nexus is the newly acquired ability of terrorist organizations to engage in criminal schemes for financial gain. Identity theft, wire fraud, stock fraud, credit card fraud, intellectual property theft, and auction fraud represent just a small sample of the potential criminal acts that terrorist networks will undertake for profit. Similar to the case of Younis Tsouli outlined at the beginning of this article, in 2011, Filipino and U.S. agents uncovered a $2 million hacking scam against AT&T that funded Lashkar-e-Taiba, the terrorist group responsible for the 2008 bombings in Mumbai, India.[37] Notably, the size of the cybercrime market is enormous, costing the global economy up to $575 billion annually.[38] Facilitated in large part by the opportunities generated through crime-terror cooperation described in the preceding section, terrorist networks will likely seek to obtain an ever larger portion of that money over time, and will do so more frequently through "in-house" capabilities.
Although less prevalent, crime-terror hybridization also takes place when organized criminals attempt to launch cyberattacks resembling acts of terror. The Economist has gone as far as to contend that organized crime groups "are the true threat to American infrastructure," citing the possibility that cyber criminals pose greater risks to national infrastructure than foreign governments.[39] The extortion of utilities through cyberattacks is a logical next step for organized

Assistant Director, Cyber Division, Federal Bureau of Investigation, 12 April 12, 2011http://www.fbi.gov/news/testimony/cybersecurity-responding-to-the-threat-of-cyber-crime-and-terrorism.

[34] John Grady, "DOJ: States, Terrorists, Team with Organized Crime Outfits to Commit Cyber Theft," *USNI News*, 29 June 2016, https://news.usni.org/2016/06/29/doj-nations-terrorists-team-organized-crime-outfits-commit-cyber-crime.

[35] Goodman, 203-206.

[36] See, for example, Barbie Latza Nadeau, "ISIS Can Buy U.K. Passports on the Deep Web to Thwart Brexit," 10 February 2017, http://www.thedailybeast.com/articles/2017/02/10/isis-can-buy-u-k-passports-on-the-deep-web-to-thwart-brexit-security.html.

[37] "Philippines say arrested hackers funded by Saudi group," *Reuters,* 26 November 2011, http://www.reuters.com/article/us-philippines-usa-idUSTRE7AP06320111126.

[38] Center for Strategic and International Studies, *Net Losses: Estimating the Global Cost of Cybercrime* (June 2014), 2, http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime2.pdf.

[39] "Organized Crime Hackers Are the True Threat to American Infrastructure," *The Economist,* 11 March 2013,

cybercrime groups searching for new business, though cyber criminals may also occasionally join in the fight to combat, discredit, or weaken trust in sitting governments.[40] To date, evidence of such activities is sparse, in part due to difficulties in attributing cyberattacks, but examples exist. In 2008, the Russian Business Network (RBN) allegedly attacked and hijacked many of Georgia's Internet servers during the Russo-Georgian conflict. Although the RBN is a recognized criminal gang, its 2008 attack appeared politically motivated and targeted public infrastructure, suggesting that the group engages not only in crime but also in terrorism through the World Wide Web.[41]

Implications for U.S. National and Transnational Security

What do the above trends in online cooperation and hybridization among criminal and terrorist groups signify for U.S. national and international security in the 21st century? Several preliminary conclusions can be drawn. First, digital environments are undoubtedly presenting new opportunities for quid pro quo exchanges and the hybridization of illicit actors, thereby making certain groups more dynamic and difficult to counter using traditional law enforcement and security measures. Criminals and terrorists have expanded access to information, tools, goods, and services that may be used to accomplish their goals, and more targets than ever before to attack. Law enforcement and national security authorities would do well to take note of these trends and monitor how illicit actors are evolving amid this reality.

Second, terrorists may particularly benefit from the crime-terror nexus in cyberspace. These groups now have new opportunities to gain knowledge and purchase resources for use toward their ideological goals, massive new opportunities for financing, and untold millions of various online targets for cyberterrorism, from individuals, to financial institutions and corporations, to national governments. International security authorities will need to closely monitor how terrorists increasingly use the Internet for operational purposes, and explore the extent to which criminals enable associated activities.

Third, these trends could present serious risks for nation-states around the world, especially to weak and developing states that are already at odds with major criminal, terrorist, or narcoterrorist organizations active within their borders. In many countries, the number of users with Internet connectivity (and thereby the number of would-be cyber criminals and terrorists) is likely to rise faster than sovereign law enforcement and judicial institutions can mature to monitor and act on illegal online activity.

Consider the case of Nigeria, where Boko Haram benefits significantly from a form of Internet fraud that entirely bypasses existing Nigerian regulatory and legal frameworks.[42] As the Nigerian case illustrates, these troubles run deep for weak and failing states, where cybercrime

http://www.businessinsider.com/organized-crime-hackers-are-the-true-threat-to-american-infrastructure-2013-3.

[40] Goodman, 24.

[41] Brian Krebs, "Shadowy Russian Firm Seen as Conduit for Cybercrime," *The Washington Post,* 13 October 2007, http://www.washingtonpost.com/wp-dyn/content/article/2007/10/12/AR2007101202461.html.

[42] David Nordell, "Boko Haram, too, is financed by cyber crime," *The Terror Finance Blog,* 18 May 2014, http://www.terrorfinanceblog.com/2014/05/boko-haram-too-is-financed-by-cyber-crime.html.

flourishes but legal restrictions remain undeveloped or poorly enforced.[43] Meanwhile, there has been explosive growth in cybercrime cases reported in recent years—India, for example, witnessed a 70 percent increase in 2014 alone—and certain nation-states may find themselves already ill-equipped to combat emerging cyber threats.[44] Governments that are unable to adequately deter these threats are at risk of losing the trust of their respective populations, weakening their legitimacy and ability to contend with illicit actors. Weak and collapsed states can further become the "breeding grounds" for those who seek to attack the United States and its allies, as home bases from which groups plan more traditional physical attacks, or outposts from which to conduct cyber-attacks or safely generate revenue online.

Policy Considerations

Further Research on the Crime-Terror Nexus in Cyberspace

To better inform policy-makers conducting threat assessments and risk mitigation strategies, scholars and security authorities alike should examine in greater depth the various components of the nexus described herein, including: (1) how terrorists derive financial, material, and operational support through online cooperation with criminals; (2) how and whether criminals seeking financial gain may tailor their online products and services to extremists as a new profitable market; (3) how terrorist organizations hybridize by regularly employing criminal tactics for ideological objectives through cybercrime and cyberattacks; and (4) how transnational organized crime groups may hybridize by carrying out major cyberattacks to aim, for instance, at destabilizing a political regime. This article is intended as an introduction to these possibilities; more in depth studies of these topics should be carried out to better inform decision makers in conducting threat assessments and risk mitigation strategies.

Strong, Cyber-Oriented, and Innovative Leadership

Forward-thinking leaders who encourage collaboration, promote awareness of threat convergence, and emphasize the broad importance of cybersecurity in law enforcement and intelligence matters are essential among today's security authorities. There are fears that some leaders in high positions within the law enforcement and intelligence communities are not technologically savvy, or even technologically disinterested. In 2012, Janet Napolitano, then head of Homeland Security and therefore all cybersecurity matters in the Department, was asked about her own cybersecurity practices. In response, she referred to herself as a Luddite and noted that she uses few

[43] Goodman, 366; Philippa Garson, "Cybercriminals find wonderland in developing countries," *openSecurity,* 10 December 2013, https://www.opendemocracy.net/opensecurity/ philippa-garson/cybercriminals-find-wonderland-in-developing-countries

[44] Government of India, "Cyber security to be ensured for the success of initiatives like 'Digital India'; says Union Home Minister," Ministry of Home Affairs, Press Information Bureau, 5 November 2015, http://pib.nic.in/newsite/PrintRelease.aspx?relid=130236.

online services and does not use e-mail "at all."[45] Today, law enforcement and intelligence agencies require leaders that, at the very least, are aware of commonly used technologies and the rapid pace of chance that they introduce to the world. Ideally, leaders who recognize the important implications of threat convergence in cyberspace can direct resources toward developing a clear organizational picture of the threat, a structured strategy to confront it, and the ability to lead analysts and agents in executing that strategy. These leaders must be prepared to strongly advocate their views on emerging threats and resist opposition from legacy institutional structures and organizational habits that adhere to outdated ways of thinking about the threats posed by criminals and terrorists in the 21st century.

International Cooperation and Capacity-Building

As terrorists and criminals can operate in cyberspace anywhere an Internet connection is available, international cooperation is essential. The United States will be decreasingly able to unilaterally monitor communications and activities in cyberspace as the number of Internet users increases overseas. In recognizing this trend, U.S. policy-makers must accept that bolstering the law enforcement and intelligence efforts of foreign counterparts will become a primary deterrent against transnational organized crime, terrorism, and the online convergence of related groups. The U.S. government should work with international partners, through foreign assistance programs that help to train and advise law enforcement agents, fortify laws and judicial institutions, and share intelligence gathering and analytical techniques in the countries that need them most. The U.S. Department of Justice's Office of Overseas Prosecutorial Development and Training (OPDAT) and International Criminal Investigative Training Assistance Program (ICITAP) should incorporate significant cybersecurity and cyber investigative components. Analogous offices in other federal investigative and foreign assistance offices, such as the State Department's Bureau of International Narcotics and Law Enforcement (INL), should follow suit.

In addition to foreign assistance programs, the U.S. government should continue to station more military, intelligence, and law enforcement attachés—especially those with cybersecurity expertise—in U.S. embassies. Attachés help build informal law enforcement and intelligence relationships that can prove tremendously useful for rapid information sharing and informal evidence exchanges. They provide the notable side benefit of promoting long-term diplomatic ties and can build the scaffolding for future, broader collaboration programs to counter illicit activities.

Mutual Legal Assistance Treaty Process Reform

Closely intertwined with legal and judicial capacity building abroad is the importance of an improved evidence-sharing framework across jurisdictions. Mutual legal assistance treaties (MLATs) govern the formal evidence-sharing process between governments, but are slow and inadequate in the digital age. MLATs are essential to the prosecution of terrorists and criminals insofar as they

[45] Josh Smith, "DHS Chief Says She Doesn't Use E-mail," *Nextgov,* 28 September 2012, http://www.nextgov.com/cybersecurity/2012/09/dhs-chief-says-she-doesnt-use-e-mail/58429/.

involve overseas activity and the need for evidence that is only available in a foreign jurisdiction. These agreements are especially relevant to the United States' relationships with foreign governments, as more crimes and terrorist acts than ever before are facilitated through Internet service providers and technology corporations like Google, Microsoft, and Yahoo, whose servers are located in the United States.[46] Significant U.S. legal protections governing access to stored communications, as well as inadequate U.S. government resources devoted to processing foreign requests for legal assistance, make popular U.S. online services even more attractive to terrorists and criminals. Foreign authorities attempting to prosecute malicious actors who have committed or facilitated criminal and/or terrorist attacks online regularly request electronic evidence from these companies, but must endure waiting periods of months to years before evidence is furnished. This is a problem that will over time impact U.S. authorities as much as their foreign counterparts; as Internet services develop abroad, the U.S. government will require ever more evidence from foreign Internet service providers to effectuate prosecutions of criminals and terrorists who target the United States and its citizens.

Employ Novel Investigative Techniques

Offline, crime-terror interactions are often uncovered by agents posing as one half of the nexus. In 2009, for example, Drug Enforcement Administration agents posed as Latin American drug traffickers and captured three individuals linked to al-Qaeda seeking narcotics trafficking protection.[47] Analogous techniques will undoubtedly prove useful in cyberspace. Given the anonymity afforded to criminal and terrorist actors in the deep web, the innovative use of undercover cyber agents and informants may be the most efficient tool in identifying and apprehending actors operating in the crime-terror realm online. Analysts and agents should study and master the use of underground communications systems, cryptocurrency, and other cyber-enabled tools to dupe would-be offenders into revealing criminal and terrorist schemes and ties.

Assess and Address Interagency Challenges

Finally, and most importantly, greater interagency collaboration is necessary to confront this threat. The online interactions described herein further confirm the idea that the fight against international terrorism is increasingly intertwined with efforts to combat transnational organized crime. A law enforcement problem can increasingly become a national security problem, and vice versa. The Congressional Research Service rightly asked in 2013 whether a specific agency or an interagency coordinating body should be designated to lead U.S. government responses to crime-terrorism threats.[48] This question is increasingly relevant today considering the role technology is

[46] U.S. Department of Justice, *FY 2015 Budget Request: Mutual Legal Assistance Treaty Process Reform*, http://www.justice.gov/sites/default/files/jmd/legacy/2014/07/13/mut-legal-assist.pdf.

[47] Richard Esposito and Jason Ryan, "Selling Drugs to Fund Terror: Al Qaeda Linked to Cocaine Trafficking," *ABC News,* 18 December 2009, http://abcnews.go.com/Blotter/selling-drugs-fund-terror-al-qaeda-linked-cocaine/story?id=9373341.

[48] Rollins and Wyler, 21.

playing in unifying and hybridizing these actors. A task force of this kind could cut through outdated organizational structures, informational silos, and bureaucratic policies that otherwise impede progress in combating threat convergence on the web. Program analysts across agencies that fight crime and terror online should compile metrics on known instances of crime-terror cooperation and hybridization, analyze trends, and assess the utility of interagency work.

To the extent that an interagency task force is deemed too costly or inappropriate to address this threat, other options exist. Interagency cybersecurity liaisons could be appointed with a mandate to study and coordinate the disruption of crime-terror activities in cyberspace. Liaisons would serve as reliable points of contact for expertise in this subject matter and to facilitate swift information sharing with other agencies as needed. Agencies may also consider coordinating interagency rotational programs that ensure agents and analysts are acquiring cross-cutting experience in a variety of departments and specialty areas. Programs of this kind would increase the number of "generalists" in relevant security agencies, which F. Matthew Mihelic describes as "necessary to maintain an organizational advantage of successful intelligence analysis in the increasingly complex situations of today."[49]

Some scholars and policy-makers may prefer to view the issues posed in this analysis from a more traditional lens—to look at cybercrime as the exclusive realm of law enforcement, for example, or to leave anything related to terrorism to counterterrorism and intelligence officials. This line of thinking ignores the changing realities of a globalizing world with a rapidly changing transnational security landscape, of which the growing crime-terror nexus is just one symptom. It is becoming increasingly important to view issues of crime and terrorism vis-à-vis one another, and the bureaucratic structures of government agencies must reflect this reality. Decision makers should pay careful attention to whether dated, compartmentalized security structures might be interfering with law enforcement's ability to adapt to online threats. A general movement toward dynamic, cross-cutting, and increasingly interlinked security authorities may be necessary to combat 21st-century threats including the crime-terror nexus.

Conclusion

While the crime-terror nexus is at times difficult to detect online, the trend is clear. Cyberspace enables broader interactions between crime and terrorism, both through cooperation between criminals and terrorists and the hybridization of criminal and terrorist organizations. National and multilateral authorities are slowly beginning to recognize these phenomena and update security paradigms to reflect online threat convergence; the European Commission's 2015 Agenda on Security prioritized "terrorism, organized crime, and cybercrime as interlinked areas with a strong cross-border dimension."[50] The findings in this article strongly reaffirm the European Commission's

[49] F. Matthew Mihelic, "Generalist Function in Intelligence Analysis," International Conference on Intelligence Analysis, McLean, VA, 2-6 May 2005.
[50] European Commission, "The European Agenda on Security," (Strasbourg: 28 April, 2015), http://ec.europa.eu/dgs/home-affairs/e-library/documents/basic-documents/docs/eu_agenda_on_security_en.pdf, 2.

report. By acknowledging this reality and exploring its intricacies in greater depth, the United States and its international partners will be better positioned to counter criminality and terrorism across the globe.