Evolving Tech, Evolving Terror

Seth Harrison

OVER THE COURSE OF THE 16-YEAR WAR ON TERROR, experts have identified political and socioeconomic conditions as root causes of terrorism. The technological enablers that make terrorism possible are less studied, however. Innovations in computing and telecommunications—like widespread internet access,[1] end-to-end encryption,[2] and virtual private network (VPN) usage[3] —have made new types of operations possible for a higher number of radicalized individuals.

The Islamic State best capitalized on the new technologically driven landscape by remotely inspiring and directing attacks.[4] These operations require little training or tactical planning, involve crude tools—like knives or cars—and can be conducted by anyone, anywhere. The combination of simple operations and increased communicative capacity has made terrorism accessible to the masses.

To date, mass-accessible operations have been confined to the West. However, as ISIS transitions to a more conventional terrorist network,[5] these attack types' geography stands to expand. As a result, policymakers would be well-served to incorporate technological conditions into their projections of emerging ISIS hotspots.

Malaysia provides an important case study in the emerging threat of remotely inspired attacks because of its widespread internet access, popular encrypted messaging services, proliferating use of VPNs, and a potential cohort of veteran foreign fighters returned from the Syrian battlefield to spur radicalized individuals into action.

Technological Capabilities

The first and most basic capability, access to the internet, has changed the way individuals radicalize and plan attacks. On the radicalization side, online platforms offer more opportunities to become radicalized and accelerate the speed with which radicalized individuals mobilize.[6] Once radicalized, jihadists have used the internet for communication and operational planning. The attack on the Curtis Culwell Center represents the most extreme occurrence, as al-Shabaab-turned-ISIS operative Mohammad Abdullahi Hassan directed the perpetrators to conduct the operation through Twitter.[7]

As with other developing countries, internet usage in Malaysia is becoming increasingly common. Sixty-eight percent[8] of Malaysians use the internet nationwide. When parsed for age, that rate climbs to 91

Policymakers would be well-served to incorporate technological conditions into their projections of emerging ISIS hotspots.

percent among Malaysians 18–34. Jihadist content producers—namely ISIS—have capitalized on the trend, targeting Malaysian youth[9] in their recruitment efforts.

Second, end-to-end encrypted messengers—like WhatsApp and Telegram—afford their users privacy by scrambling data[10] sent from the sending device, through the cell tower and server, to the receiving device. In terrorist applications, these encrypted messaging services allow for unprecedented operational security, limiting law enforcement's ability to view or disrupt these communiques.

Encrypted messaging is surprisingly popular in Malaysia and represents three of the top twenty-five[11] most popular mobile applications in the country. Violent extremists can leverage this fact, employing the technology to plot domestic operations.

Finally, in the same way that prospective terrorists use encrypted messaging for offense—to stage attacks—VPNs allow radicalized individuals to play defense. As their name suggests, VPNs provide users with a private connection to the internet, replacing the user's Internet Provider address with one from a VPN provider. In doing so, the technology effectively anonymizes the internet activity of the user. For terrorists, this prevents law enforcement from tracking their movement and intentions.[12]

In Malaysia, VPN usage outpaces most Western countries. Approximately one in three[13] internet users anonymize their online presence. The reasons for VPN usage vary: popular rationales in Malaysia range from accessing free entertainment to hiding web browsing from the government. This existing VPN culture can readily turn sinister and the technology applied to jihadist activity.

Terrorist Intent

Malaysia's technological landscape is necessary but not sufficient for operations with low technical barriers. Terrorist intent in the country is required for ISIS to ramp up its activity. Here, both internal and external pressures have resulted in populations who may use technology to conduct terrorist operations.

Despite the geographic distance between Malaysia and the Syrian Civil War, returning Malaysian foreign fighters from the conflict stand as a concern to policymakers. Though estimates vary wildly, as many as 400 Malaysians[14] entered the conflict zone in Syria and Iraq. Further, eight confirmed cases[15] of foreign fighters returning to Malaysia highlight the threat's viability. This number stands to grow, as Malaysian security services reported that Turkey has been deporting non-Malaysian foreign fighters to Malaysia.[16]

Internal changes to Malaysian society exacerbate the terrorist threat. Malaysia is beginning to embrace more conservative religious practices[17] and politically this is spurred by Malaysia's ruling United Malays National Organization (UMNO) party. This process has the dual effect of normalizing conservative interpretations of Islam for some, and generating public distrust of the government for others. In the latter case, this distrust may further propagate VPN use among large segments of the population—a dynamic that extremists can tap into. Further, ISIS has specifically targeted Malaysia with Malay-language propaganda.[18] These dynamics have translated into real action: the Royal Malaysian Police (RMP) have disrupted at least 14 ISIS-related plots.[19]

Recommendations

In Malaysia and similarly positioned countries, some have advocated for stronger key disclosure laws,[20] which compel suspects to surrender their passwords. In many cases, however—as with the San Bernardino attack[21]—the keyholders are deceased. Others have called for telecommunication companies to build backdoors[22] into their products, which would give law enforcement a way to access encrypted data. Although methods for VPN blocking exist, VPNs remain largely unregulated internationally.

These policy options all attempt merely to disrupt the technology's distribution but do little to undermine the technology itself. In other words, VPNs and encryption can exist without VPN and encrypted messaging providers—especially in the context of illicit activity. As a result, policymakers must look elsewhere to combat the threat.

More promising approaches involve placing a renewed emphasis on defensive counterterrorism measures. While continuing to work to prevent attacks, law enforcement should also explore new ways to mitigate attacks' effectiveness. Examples of this thinking have begun to emerge in Europe, where new barriers[23] will limit the impact of vehicular rammings.

While the government's ability to disrupt accessible terror is limited, it can consider the availability of these technologies as a factor in determining high-risk locations. This increased awareness can be used to better target preventative efforts and assist officials in finetuning their threat assessments.

Conclusions

In the recent months, counterterrorism policy conversations have become increasingly politicized. For some, terrorists are irredeemable and counterterrorism strategy should be driven by kinetic force. Others maintain that counterterrorism strategy should focus on the root causes of terror. In the past, counterterror policy has largely remained immune from the divisive political discourse that has plagued other public policy issues. If counterterrorism's technocratic character is to continue, apolitical approaches to counterterrorism will be required.

Careful analysis of the technological enablers of terrorism fits squarely into this model. It captures both tactical and strategic considerations warranted by emerging technologies and, favoring more defensive approaches, occupies space far enough downstream to sidestep counterterrorism's thornier political questions. It remains clear, however, that as more people gain access to more sophisticated technologies, counterterrorism efforts will have to adapt.

Seth Harrison is a research intern with the Transnational Threats Project at CSIS.

Endnotes

[1] Michael Steinbach, “ISIL Online: Countering Terrorist Radicalization and Recruitment on the Internet and Social Media,” Statement before the Senate Committee on Homeland Security and Governmental Affairs, Permanent Subcommittee on Investigations, July 2016, Washington, DC, https://www.fbi.gov/news/testimony/isil-online-countering-terrorist-radicalization-and-recruitment-on-the-internet-and-social-media-.

[2] Robert Graham, “How Terrorists Use Encryption,” *CTC Sentinel*, Vol. 9.6, 2016, https://ctc.usma.edu/posts/how-terrorists-use-encryption.

[3] EUROPOL Public Information, “Changes in Modus Operandi of Islamic State Terrorist Attacks,” The Hague, January 18, 2016.

[4] Rukmini Callimachi, “Not ‘Lone Wolves’ after All: How ISIS Guides World’s Terror Plots from Afar,” *New York Times*, February 4, 2017, https://www.nytimes.com/2017/02/04/world/asia/isis-messaging-app-terror-plot.html?mtrref=t.co&gwh=EF42D2AC6FBB561AE4B61F3E3FB71270&gwt=pay.

[5] C.P. Clarke, “How ISIS Is Transforming,” RAND Corporation, September 25, 2017, https://www.rand.org/blog/2017/09/how-isis-is-transforming.html.

[6] I. Von Behr, A. Reding, C. Edwards, and L. Gribbon, *Radicalisation in the Digital Era: The Use of the Internet in 15 Cases of Terrorism and Extremism*, RAND Corporation, 2013, https://www.rand.org/content/dam/rand/pubs/research_reports/RR400/RR453/RAND_RR453.pdf.

[7] R. Callimachi, “Clues on Twitter Show Ties between Texas Gunman and ISIS Network,” *New York Times*, May 11, 2015, https://www.nytimes.com/2015/05/12/us/twitter-clues-show-ties-between-isis-and-garland-texas-gunman.html.

[8] J. Poushter, “Smartphone Ownership and Internet Usage Continues to Climb in Emerging Economies,” Pew Research Center, February 22, 2016, http://www.pewglobal.org/2016/02/22/smartphone-ownership-and-internet-usage-continues-to-climb-in-emerging-economies/.

[9] M. Mohd Sani, *ISIS Recruitment of Malaysian Youth: Challenge and Response*. Middle East Institute, May 3, 2016, http://www.mei.edu/content/map/isis-recruitment-malaysian-youth-challenge-and-response.

[10] Graham, “How Terrorists Use Encryption.”

[11] “Follow the Leaders: Highest Ranking Apps in Apple App Store, Malaysia,” Similar Web, https://www.similarweb.com/apps/top/apple/store-rank/my/all/top-free/iPhone.

[12] EUROPOL Public Information, “Changes in Modus Operandi of Islamic State Terrorist Attacks.”

[13] “How VPN Use Varies by Country,” *Wired*, http://www.wired.co.uk/gallery/vpn-use-varies-by-country.

[14] R. Barrett, *Beyond the Caliphate: Foreign Fighters and the Threat of Returnees*, Soufan Center, 2017, http://thesoufancenter.org/wp-content/uploads/2017/10/Beyond-the-Caliphate-Foreign-Fighters-and-the-Threat-of-Returnees-TSC-Report-October-2017.pdf.

[15] Ibid.

[16] K. Craigin, “Foreign Fighter ‘Hot Potato,’” Lawfare, December 26, 2017, https://www.lawfareblog.com/foreign-fighter-hot-potato.

[17] D.F. Fernandes, “Malaysia's Slide toward More Conservative Islam,” *The Diplomat*, October 4, 2017, https://thediplomat.com/2017/10/malaysias-slide-toward-more-conservative-islam/.

[18] J.C. Liow, “Malaysia's ISIS Conundrum,” Brookings Institution, July 28, 2016, https://www.brookings.edu/opinions/malaysias-isis-conundrum/.

[19] “Special Branch Drop IS Bombshell, Reveal 14 Attack Attempts in Malaysia Foiled,” *New Straits Times*, December 6, 2016, https://www.nst.com.my/news/2016/12/194965/special-branch-drop-bombshell-reveal-14-attack-attempts-msia-foiled?m=1.

[20] T.J. Holt, A.M. Bossler, K.C. Seigfried-Spellar, *Cybercrime and Digital Forensics: An Introduction* (Abingdon, Oxon: Routledge, 2018).

[21] B. Bergstein, “What If Apple Is Wrong?,” *MIT Technology Review,* May 20, 2016, https://www.technologyreview.com/s/601145/what-if-apple-is-wrong/.

[22] B. Barrett, “The Encryption Debate Should End Right Now,” *Wired*, June 30, 2017. https://www.wired.com/story/encryption-backdoors-shadow-brokers-vault-7-wannacry/.

[23] N. Robins-Early, “London Deploys the ‘Talon’ to Thwart Car-Ramming Attacks,” *Huffington Post*, September 11, 2017, https://www.huffingtonpost.com/entry/london-car-ramming-attack-terror_us_59b68f88e4b0354e441344e2.