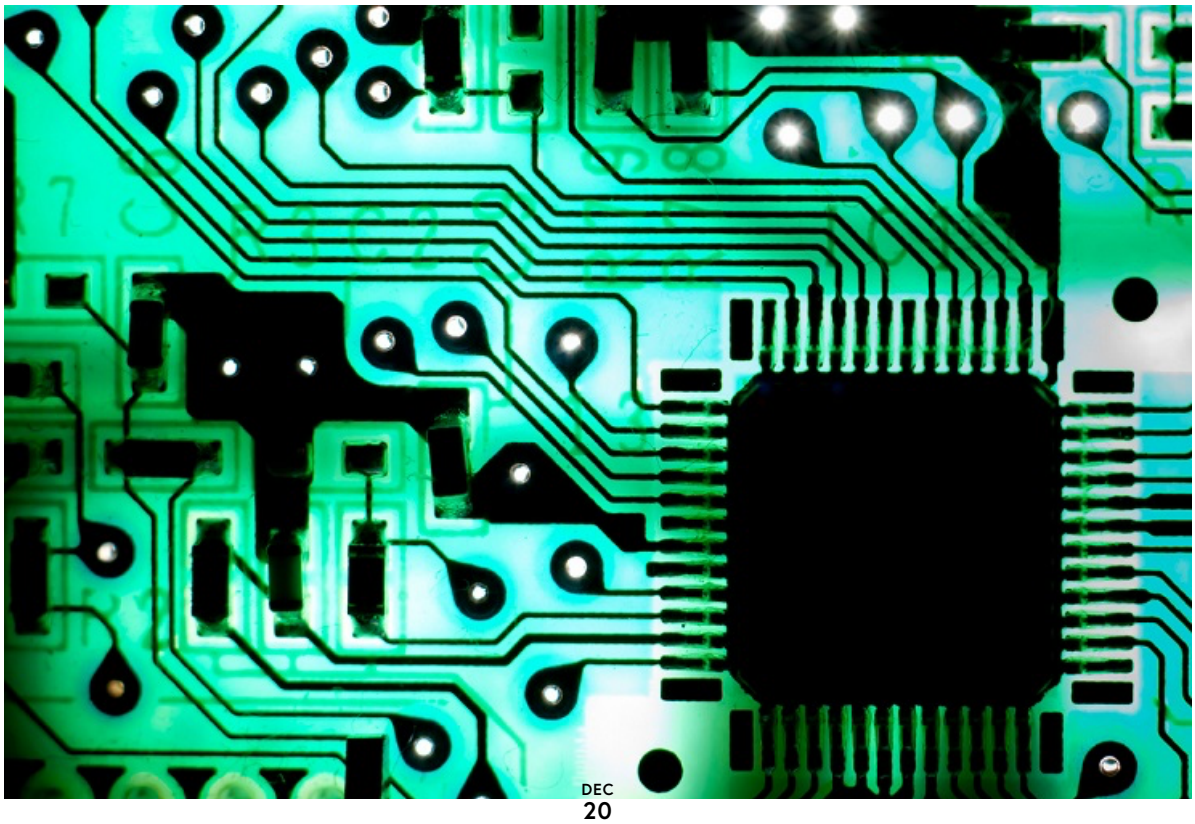
The Fletcher Forum of Wo



DEC
20

#Tech4Terror vs. #Tech4Good

SECURITY (/HOME/CATEGORY/SECURITY), BUSINESS AND FINANCE (/HOME/CATEGORY/BUSINESS+AND+FINANCE), SCIENCE AND TECHNOLOGY (/HOME/CATEGORY/SCIENCE+AND+TECHNOLOGY)

by **Aaron Brantly**

Communications, commerce, art, and society have been dramatically influenced by technology in the last 50 years. An iPhone 6 is approximately 120 million times faster than the computer used in the Apollo missions. Technology is and will continue to shape

how we live our lives. Just as this technology can help us to land on the moon, map the human genome, and allow us to FaceTime with our friends and family, it can also be used to engage in criminal and terroristic activities designed to harm us.

Over the last year, a colleague and I have been immersed in jihadist forums and propaganda. Our foray down the rabbit hole of jihadist propaganda and digital operational security began when my colleague started noticing requests for technical support become increasingly prevalent within the forums. We released our initial analysis of jihadist technical support in TheSentinel (https://www.ctc.usma.edu/posts/extremist-forums-provide-digital-opsec-training) in May 2015. Since May, we have watched as jihadists—specifically those with an interest in helping the so-called Islamic State (ISIS)—diversify and intensify their efforts to provide a robust set of tools to evade law-enforcement and intelligence agencies.

Our article, which was shared with the National Counter Terrorism Center and other agencies, initially raised a few eyebrows, but largely fell off the public radar. When the Paris attacks occurred in November, many analysts speculated that the jihadists had used encrypted communications to plan and carry out their attacks. NBC News found our article from May and dubbed the broad network of jihadi platforms and communications on digital operational security the "Jihadi Help Desk (http://www.nbcnews.com/storyline/paris-terror-attacks/isis-has-help-desk-terrorists-staffed-around-clock-n464391)."

In many ways, the decentralized platforms and communications methods—including Telegram, Signal, al-Minbar al-I`lami al-Jihadi, Shmukh al-Islam, and Al-Fida'used—used by jihadists across the globe to evade law enforcement and intelligence agents, when taken together, resemble a typical computer help desk at a university or corporation. However, there is no phone number or single individual to turn to at all times. What we found instead were several

recurring usernames who logged on and off at different times across different platforms. These individuals and other users posted and answered questions, providing both homegrown and co-opted content.

The level of sophistication associated with the questions ranged from the technologically mundane (e.g. whether Skype is secure) to the technologically complex (e.g. how to root an Android phone to direct all of its data traffic through the anonymizing software, Tor). Recommendations and answers to questions came in multiple forms including forum posts, chat logs, PDF documents, JustPaste.it (http://justpaste.it/), Dump.To, tweets, YouTube, and Vimeo videos comprising more than 300 pages of training documents on the use of more than 120 different tools. Many of the materials and tools used to train and facilitate extremist actions were lifted straight out of democracy and human rights training manuals from well-intentioned organizations.

The innovative uses of technology that we and others have identified enable ISIS to recruit, propagandize, plan, and engage in terrorist operations globally. Combined, the distributed platforms that provide jihadist training materials indicate an organizational and capacity development process in line with established theoretical works. These include Sarah Parkinson's work on "Organizing for Rebellion (http://journals.cambridge.org/action/displayAbstract?fromPage=online&aid=8963083)" and Marc Sageman's concepts of organizational development under a leaderless jihad (http://www.upenn.edu/pennpress/book/14390.html).

As anyone who works in the information technology industry knows all too well, organizations are constantly trying to enhance their security practices. Most corporations, government entities, and universities mandate cybersecurity trainings on a regular basis to safeguard intellectual property, personally identifiable information, and other data types now crucial to economic and social life. Despite extremists' efforts to advance their own digital

security, the reality is that their innovation and adaptation is not fait accompli. As most administrators know, individuals across industry, academia, and government consistently fail to implement even the most basic security precautions on a regular basis; the same is true of transnational terrorists.

As organizations like ISIS, al-Qaeda, and others work to strengthen their organizational capacity, it should not come as a surprise to anyone that they use the Internet to advance their goals. However, it should also not be a surprise that while they utilize these tools and explicitly train on encrypted communications, a very large percentage of individuals will fail to adequately utilize encryption. Most will fail to use it because to do so is often an inconvenience, while others will fail to use encryption properly simply because it is hard to use effectively at all times. When they do fail to secure their devices and communications, as they regularly do, they are far more easily tracked.

Organizations like the National Democratic Institute, the Guardian Project, the Tor Project, the Open Technology Fund, and Cyberkov are vital to efforts to protect human and democracy rights activists, journalists, and other vulnerable groups around the world through the use of encryption, proxies, and tools to remove digital footprints. Although their work is often co-opted by nefarious groups such as criminals and terrorists, this does not obviate the value and importance of the aforementioned organizations in advancing human rights and a free press.

Moreover, the use of encrypted communications by groups and individuals who seek to do harm is not sufficient justification for arguments to undermine the mathematics of encryption technologies in either the private or public sector. The proper and legitimate use of encryption technologies underpins human rights, freedoms of the press, and the economics of daily life. To introduce deliberate vulnerabilities for the purpose of hindering nefarious activity is at best a stopgap measure that assumes terrorists and criminals are

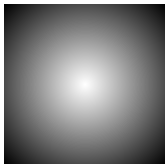
unwilling to innovate in response to changes in legislation. At worst, it adds new avenues to exploit the infrastructure upon which we depend every day.

Terrorists innovate and adapt. Technology can be used for good and it can be used for bad. We have identified an instance of its use for the latter, but that should not detract from its immense potential to advance the former.

The views expressed here are those of the author and do not reflect the official policy or position of the Department of the Army, Department of Defense, or the U.S. Government.

Image "Algorithmic Contaminations (https://www.flickr.com/photos/derekgavey/5528275910/)" Courtesy Derek Gavey / CC BY 2.0 (https://creativecommons.org/licenses/by/2.0/)

About the Author



Aaron F. Brantly, Ph.D., is Assistant Professor of International Relations and Cyber in the Department of Social Sciences at the United States Military Academy, Cyber Policy Fellow for the Army Cyber Institute, and Cyber Fellow at the Combating Terrorism Center.

‹

Dec 21 Challenges and Opportunities for Chinese Investment in the U.S.

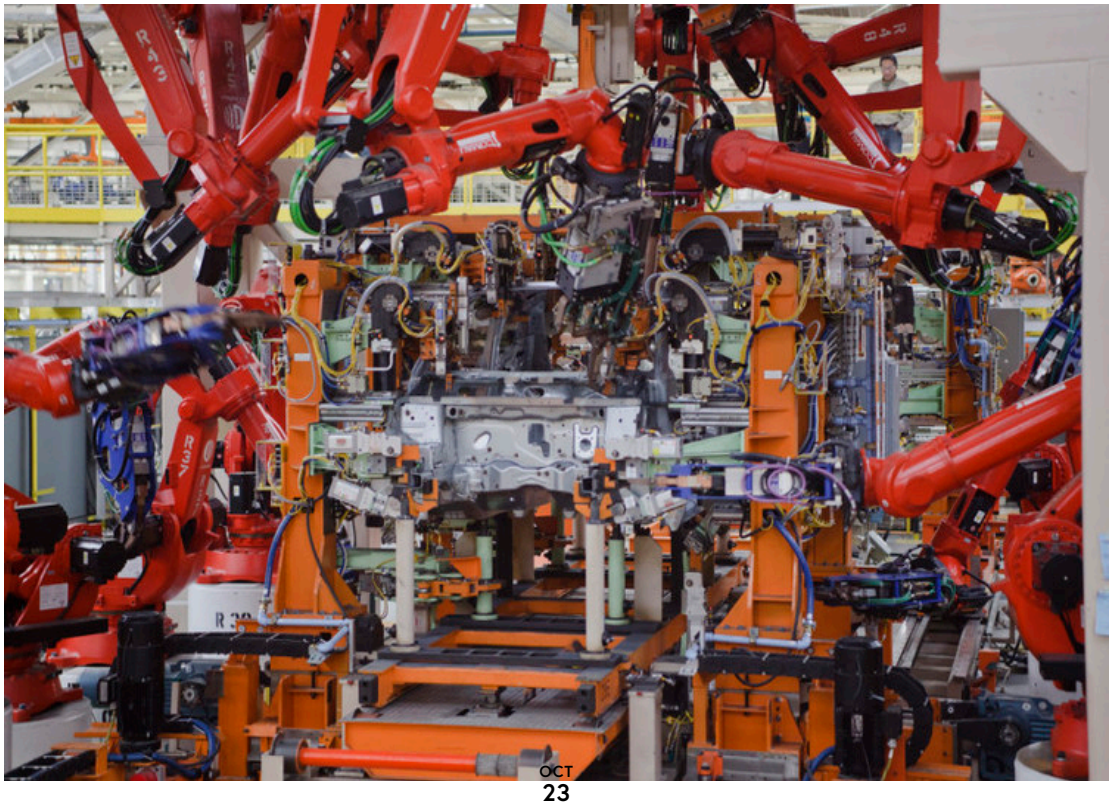
(/home/2016/8/1/challenges-and-opportunities-for-chinese-investment-in-the-us)

❯

Dec 19 Why Was China's Response to U.S. South China Sea Patrols So Mild?

(/home/2016/9/6/why-was-chinas-response-to-us-south-china-sea-patrols-so-mild)

Related Posts



OCT
23

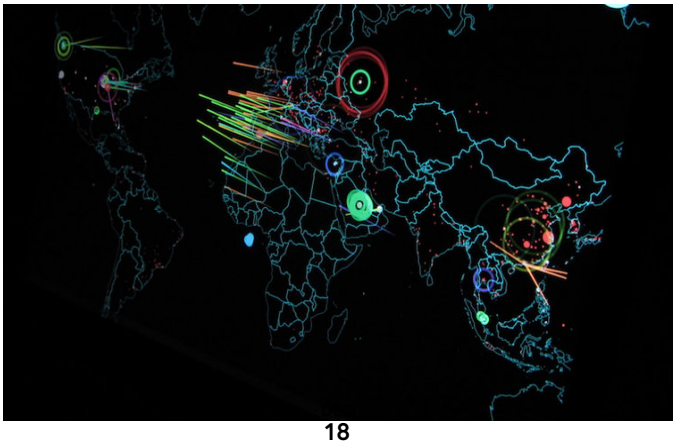
Global Development in the Age of Automation: Catapult or Detour?

(/home/2016/8/1/global-development-in-the-age-of-automation-catapult-or-detour)

JAN
13

A Chinese Ministry of Love?

(/home/2016/8/12/a-chinese-ministry-of-love)



18

Toward a Global Cyberspace Regime

(/home/2016/8/12/toward-a-global-cyberspace-regime)

SUBMIT TO THE FLETCHER FORUM (HTTPS://FORM.JOTFORM.COM/FLETCHERFORUM/SUBMIT)