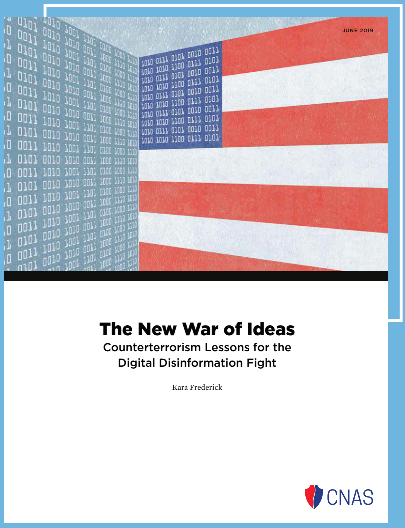
التحالف الإسلامي العسكري لمحاربة الإرهاب
ISLAMIC MILITARY COUNTER TERRORISM COALITION

International Reports

14

THE NEW WAR OF IDEAS

Counterterrorism Lessons for the Digital Disinformation Fight



JUNE 2019

The New War of Ideas

Counterterrorism Lessons for the Digital Disinformation Fight

Kara Frederick

CNAS

June 2020

www.imctc.org

التحالف الإسلامي العسكري لمحاربة الإرهاب
ISLAMIC MILITARY COUNTER TERRORISM COALITION

International Reports

Monthly Issue - General Directorate of Planning and Coordination

Director General

Major General Mohammed bin Saeed Al-Moghedi
Secretary-General of the Islamic Military Counter-Terrorism Coalition

Editor-in-Chief

Colonel Hassan bin Suliman Al-Amri
Director of the General Directorate of Planning and Coordination

Brought to you by

TAOQ RESEARCH

TAOQ توق

E-mail: info@taoqresearch.org
Phone: +966 114890124

International Reports
14

June 2020

THE NEW WAR OF IDEAS
Counterterrorism Lessons for the Digital Disinformation Fight

The ultimate goal of this study by Kara Frederick is to fight back against a spate of malign foreign influence campaigns, digital disinformation and hacking attempts. She emphasizes at the beginning of her study that the future of the world order hinges on influencing peoples. This is true as long as civilians have long been the currency of bitter conflict across the scale from insurgencies through terrorism up to information war operations. It is the emerging technologies that revolutionize the rules of the influence game. Glaringly, the advances notched up in artificial intelligence (AI), particularly machine learning, weaponize information to wield social control at scale. More so, authoritarian regimes, such as China and North Korea, have taken advantage of new technologies to tighten their firm hold over their peoples, instrumentalizing state-controlled social media which is kept under surveillance, automated application networks, and facial recognition technology.

Attempts to Undermine Trust

Foreign actors are always attempting to undermine and erode public trust in democratic pathways propelled through computational propaganda and microtargeting. Sadly enough, non-state actors are also stoking and arousing political tensions through the dissemination of disinformation online. Such attempts often target and aim at the existing liberal regime and the associated support institutions and bode ill for potential geopolitical upheavals. Hence, Frederick drops a subtle reference to a blueprint to resist this threat, which draws on and exists in the lessons of entering a different war. Following the 9/11 Attacks, counterterrorism has offered a roadmap for both public and private organizations on how to respond to a new yet different battlefield; it is information battlespace.

In full recognition of the existing and potential terrorist threats, the US government along with the private businesses set the tone to contest such terrorist threats in physical and digital channels and landscapes. Between 2002 and 2017, the level of seriousness and intensity of the US government was felt in the cost paid for the global war on terrorism by the US; it cost approximately $2.8 trillion in related expenditures, making up about 16% of discretionary spending during the same period of time. This is the price paid for a strategy to disrupt and nip terrorism in the bud before it strikes home, as the US military counters terrorism in its safe havens abroad.

The Impact Sustained by Social Media Companies

New media companies and social media platforms have formed a solidarity group to counter terrorism, especially after Daesh claimed to publish a video clip of beheading American journalist James Foley on YouTube and Twitter in 2014, opening a new front for companies. By 2015, Facebook, which was against counterterrorism legislations aimed at uprooting terrorist progress, held several meetings with other technology companies to discuss the idea of a platform to counter terrorism. In early 2016, White House officials and other officials went to Silicon Valley to meet senior technology leaders, led by Apple CEO Tim Cook and representatives of Google, Facebook, Yahoo and Twitter, to further discuss developing solutions to curb the spread of terrorist content on the internet.

In the same year, Alphabet Incorporation Jigsaw helped to counter Daesh tactics over the internet and filtered the content on YouTube. The idea of creating that incubator is attributed to Google. By 2018, Facebook hired 7,500 employees as content managers, and one of their primary job tasks was to keep the social platform free from terrorist content. In the three years following those initial discussions in 2015, Twitter suspended 1.2 million accounts of subscribers who violated counterterrorism policies.

As the tone was to start the war on terrorism, technology companies began to work actively against their platforms for terrorism actors. Such companies hired talent to fill gaps and enhance expertise in combating terrorism, creating new positions to coordinate and oversee the global counterterrorism regulations. They contracted with relevant stakeholders in the internal forums, and established a set of technical measures and important analyses to root out the malign content and the abusive user. Large and small technology companies have cooperated with each other and with law enforcement in exchanging any information related to security threats, and have drafted regulations to prevent terrorism from abusing their digital platforms in particular.

Means of Foreign Influence Campaigns

1. Disinformation

Influence campaigns that rely heavily on propagating disinformation can be defined as the organized use of information to intentionally confuse, mislead or shift the public opinion to a targeted group of people to achieve strategic goals. To resist and combat the efficiency of this type of disinformation, we should pay special attention to agents or actors, and to enablers such as tools and mechanisms for digital misinformation campaigns and foreign influence.

Means of Foreign Influence Campaigns

1 Disinformation
2 Amplification
3 Spear-Phishing
4 Hacking

As for agents or actors, researchers, the media and public opinion continue to draw attention to the influence campaigns sponsored by some countries by leading authoritarian forces ideologically opposed to democracies. For instance, the Russian use of influence operations to undermine transatlantic solidarity is well documented.

As for the elements of empowerment, actors can combine the tactics of amplification and microtargeting to increase their influence to the maximum extent possible. In assessing online robot activity conducted in 2016 by American cybersecurity, robots accounted for more than 50% of online traffic. Political robots target public opinion by amplifying destructive or damaging stories by 'troll farms' of internet users coordinating their posts with other users with the intent to harass, mislead and broadcast disinformation, using social media robots, which are automated networks of fake accounts.

2. Amplification

The amplification of political polarization is one of the means of foreign influence campaigns as it provides ample opportunities for foreign entities to divide the American public. For instance, in the aftermath of the 2018 Parkland High School shooting, Russia sought to stoke the debate in the US about the absence of arms control laws, by flooding Twitter with controversial comments under incendiary hashtags of gun control laws to elicit more emotional reactions. The low protection barriers on social media and new media make it easy for malicious actors to access false or biased content and to broadcast organized propaganda that mess with the information environment. A research study conducted by the Massachusetts Institute of Technology (MIT) in 2018 revealed that the spread of disinformation on Twitter is faster and more tangibly deeper than the spread of the truth.

3. Spear-Phishing

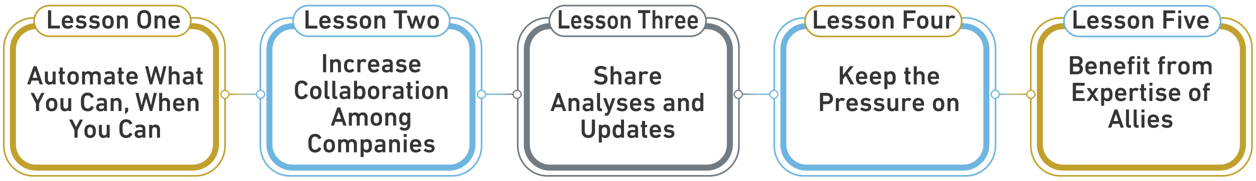
Characteristically, spear-phishing is a set of attempts to trick and fool a target people into revealing information or rather installing malware programs through a legitimate request by email. Examples of digital spear-phishing include the email-based attack that victimized John Podesta, chairman of presidential candidate Hillary Clinton's campaign, and the Democratic National Convention in 2016. With the help of AI-powered information processing, these attacks will become more difficult to distinguish from legitimate and true inquiries.

Foreign influence campaigns use another type of "disinformation", which is Seeding false information into a stream of hacked, real information, which can undermine trust in electoral candidates themselves. For instance: During the French election campaign of President Emmanuel Macron, in 2017, an incident was considered a realistic field test for this technique. Russian operatives reportedly forged documents to "bear evidence and prove" that one of Macron's staff purchased drugs. The Russians then mixed in and concocted falsified documents with hacked authentic information, hoping to turn French public opinion against Macron and his team at the time.

4. Hacking

Foreign influence campaigns strike the infrastructures of traditional election processes, specifically before 2016. According to New York University's Brennan Center, 43 states used old

Lessons from Muscle Memory



Lesson One
Automate What You Can, When You Can

Lesson Two
Increase Collaboration Among Companies

Lesson Three
Share Analyses and Updates

Lesson Four
Keep the Pressure on

Lesson Five
Benefit from Expertise of Allies

voting machines prone to malfunction and reliant on obsolete and unsafe software in 2016. In the same vein, similar inspections also revealed serious vulnerabilities with US voting machines, including devices connected to a wireless network that was easily accessed with mobile phones and voting machines with potential vulnerabilities in ballot counting processes.

Lessons from Muscle Memory

Modern digital technologies pose a new set of vulnerabilities, opening up new pathways for cognitive and digital subversion. Technology companies and the public sector possess the muscle memory for identifying such attempts, restricting the space in which malign actors operate, while fighting back against associated initiatives. The counterterrorism experience created this muscle memory, which can be summed up in five lessons.

Lesson One: Automate What You Can, When You Can

First, social media companies should block the space in which foreign actors conduct malicious actions, by raising the readiness of their platforms to be "hostile" to terrorist content, and then apply defensive methods to effective state-sponsored campaigns. Restricting the actions taken by foreign influence campaigns, such as those conditions that Facebook operates as a "coordinated behavior", companies can adopt specific measures in this context, including reducing the use of nicknames and anonymities, and relying on strict steps to verify identity, such as checking accounts that show more automated than human indicators and behaviors, and assessing the integrity of the accounts. Google and Facebook implement similar measures to address and counter ways of spreading disinformation.

Twitter suspended 70 million accounts in May and June of 2018. As the volume and variety of data increases in the information environment, applying automation and machine learning to content mitigation, reducing amplification and tightening attribution, the opportunities of attackers to access the internet space will be less.

Lesson Two: Increase Collaboration Among Companies

The challenges sustained by relevant companies are often shared challenges in this new global battle, hence taking unified appropriate actions unanimously is very important. For example, Facebook has imposed new regulations and advanced technologies, the application of which exceeds the US and Canada to millions of users in the world.

In September 2018, Facebook Chief Operating Officer Sheryl Sandberg told the Senate Intelligence Committee that Facebook is working closely with industry peers to make progress in tackling the problem of foreign influence campaigns. In the same month, Google, Facebook and Twitter pledged to work together to fight false information and disinformation in Europe, which is a test for generalizing the experience and expanding this cooperation globally.

Lesson Three: Share Analyses and Updates

One of the fundamental components in combating malicious networks and their agents to which we should pay a special attention is how to organize for the battle or fight. Since technology is a major factor in future wars, relying on past achievements

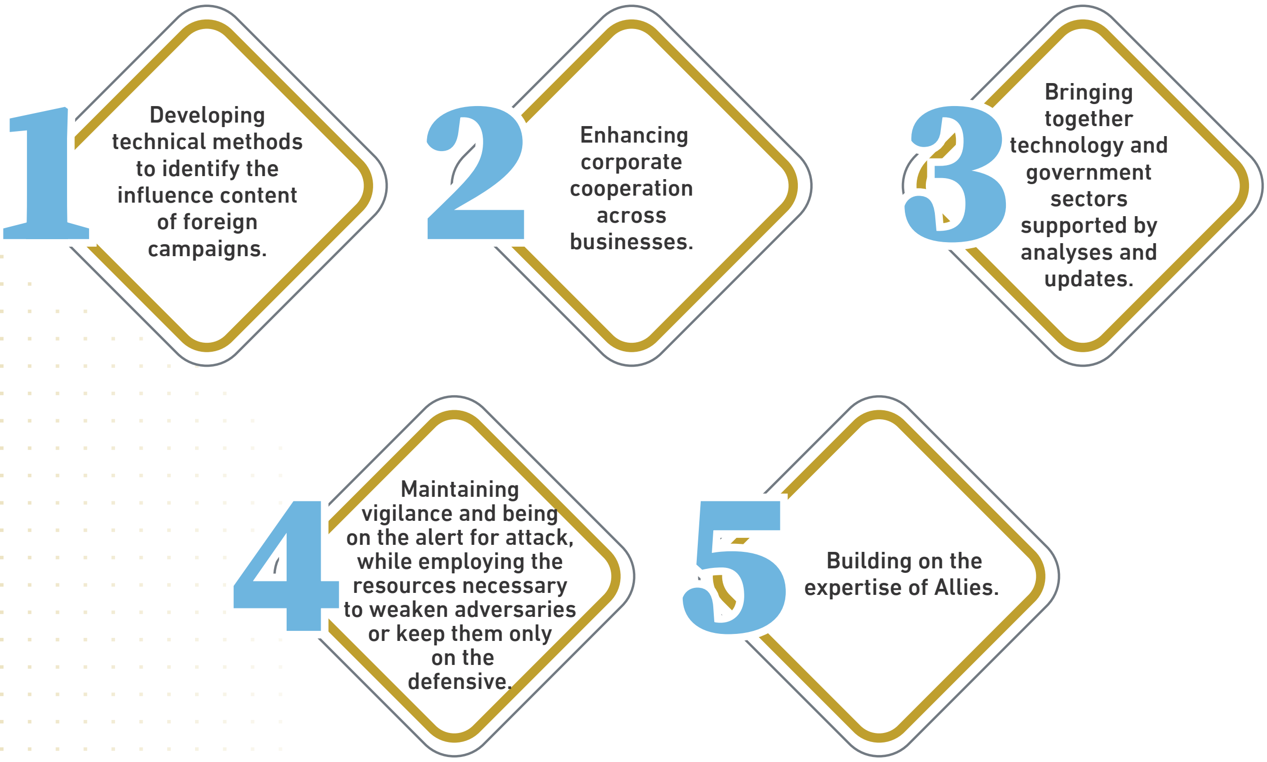
can bridge the gap between the public and private sectors, through experts who share common goals. These frameworks and integration systems do exist, and they can be measured. For example, the National Center for Counter-Terrorism was established in North Virginia in 2004 to improve the information-sharing system, and to improve predictive capabilities and rapid response to terrorist threats. As such, experts suggest simulating the idea, and creating a similar institution, with the same function, to counter foreign influence processes.

The recommendations state the necessity of appointing a body comprising members of the intelligence agency to combat terrorism, in close coordination with the private sector, to create smaller cells, more likely to move and integrate easily, under its supervision and financing, and to deal digitally with malicious foreign influence campaigns. More so, social media companies should pay special attention to these efforts, and provide these small cells with the expertise of their counterterrorism analysts.

Lesson Four: Keep the Pressure on

More sustained pressure needs to be made, despite the good performance of the government and technology companies; however, terrorists will continue to find innovative methods of societal abuse, through social media platforms and new media, and social media companies will continue to hire counterterrorism analysts and auditors. While the ability to transfer these tools to combat terrorism and technologies provides a useful springboard, the problem of disinformation and its broad implications for democratic institutions impose an urgent need to continuously take a proactive position.

Mendacity, disinformation and influence campaigns benefit dictatorships, which rule by power and intimidation, while truth is a touchpoint, a disinfectant against corruption and tyranny in free societies. Some regimes find themselves forced to cloak reality with mendacity to maintain power, as is the case of the harmonious society of North Korea or China that controls the strict regime. On the other side, we find democracies that give people



1 Developing technical methods to identify the influence content of foreign campaigns.

2 Enhancing corporate cooperation across businesses.

3 Bringing together technology and government sectors supported by analyses and updates.

4 Maintaining vigilance and being on the alert for attack, while employing the resources necessary to weaken adversaries or keep them only on the defensive.

5 Building on the expertise of Allies.

access to the truth. When authoritarian regimes are based on mendacity to tighten their hold, then this weaponizes truth in the face of repression, and the US should not give up this advantage. When truth prevails, democracy triumphs.

Lesson Five: Benefit from Expertise of Allies

All efforts and strategies are based on an important advantage, not invested as required; namely, the US democratic allies. NATO contributions to the war on terrorism have strengthened intelligence collection and have driven operations in Operation Enduring Freedom in Afghanistan. NATO became an official member of the Global Coalition to Defeat ISIS in May 2017, and a member of the Intelligence Terrorism Intelligence Cell, which is based and headquartered in Brussels. In the face of security threats in Afghanistan, 38 countries, as well as the US, supply troops to Operation Resolute Support in Afghanistan to counter the terrorist threat.

Summary

Following the 9/11 Attacks, the war on terrorism veered off; a new stage of counterterrorism has occupied the foreground and hence has come into play, affecting the US technology companies. Frederick further explains: "Today, the US is participating in an expansionist struggle that requires the intervention of the main influence actors themselves in the technology companies in the private sector and the US government. They can no longer afford to repeat the mistake, and miss many of the lessons learned over two decades in fighting terrorism, in strategic, technical and organizational terms." Building on successful experiences in the technology sector and the US government counterterrorism efforts enhances the ability of the US to challenge digital disinformation in the future.

Recommendations

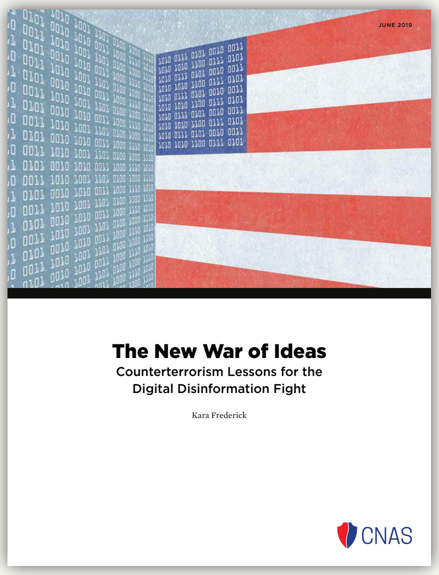
- In the long run, technology companies should direct a permanent percentage of their engineering power to automate the research for the identity of malign influence campaigns. Companies can gain significant leverage by exploiting practices and traditions in applications, such as a hackathon event on Facebook by meeting computer programmers to exchange engineering experiences and missions.
- Technology companies should establish and finance an association specialized in disinformation to join the companies created after the Global Internet Forum for Combating Terrorism (GIFCT).
- The Office of the Director of National Intelligence (ODNI), in close coordination with the private sector, should designate a body of agency representatives to create smaller, more progressive, and financing merging cells that bring together public and private sector analysts. New media or social media companies are required to take advantage of their employees, who work on analyzing intelligence threats, with intelligence agencies to provide analyses to this body, and to open a continuous dialogue, while adhering to what suits each dialogue from the levels of secret and non-secret classification. When signs of success are shown, the US government should consider allocating an independent force.
- The executive authority should expand the strategy of cybersecurity, and the powers of the American cyber leadership, by carrying out offensive operations that cause losses to opponents.
- The US government should work with its democratic allies to exchange practices and experiences in clamping down on foreign influence campaigns, while building on their expertise to take offensive cyber measures.

The Author

Kara Frederick spent six years as a counterterrorism analyst at the Department of Defense and served as a senior intelligence analyst for a US Naval Special Warfare Command. She contributed to the formation of the first global cyber security team at Facebook, and served as the leader of the regional investigation team at Facebook headquarters in California. She is the Associate Fellow for the Technology and National Security Program at the Center for a New American Security (CNAS). She received her MA in War Studies from King's College London and her BA in Foreign Affairs and History from the University of Virginia.

THE NEW WAR OF IDEAS

Counterterrorism Lessons for the Digital Disinformation Fight



JUNE 2019

The New War of Ideas

Counterterrorism Lessons for the Digital Disinformation Fight

Kara Frederick

CNAS

التحالف الإسلامي العسكري لمحاربة الإرهاب
ISLAMIC MILITARY COUNTER TERRORISM COALITION

التحالف الإسلامي العسكري لمحاربة الإرهاب
ISLAMIC MILITARY COUNTER TERRORISM COALITION