# 1

# Cyber Operations

## 1.1 Cyber Operations Introduction

Cyber operations include the collection of data. This collecting of information is an enduring activity that existed long before cyber (Crumpton, 2012). However, with the advent of networked persistent memory devices (e.g., personal computers, and iPhones), using technology to access "end points" and exploit resident data became both a viable alternative to conventional spying and a new, usable tradecraft.

### 1.1.1 Cyber – A 21st-Century Collection Channel

One of the key issues inspiring the recent increase in the use of cyber, as a collection channel, is the volume of information that can be collected by cyber means. For example, a Cold War spy's ability to move information, even with the most advanced collection and data transfer techniques, likely peaked on the order of kilobytes, megabytes at best, of information transfer. With the current capacity of cyber storage and communication, however, terabyte downloads are common for commercial attacks (Warner, 2017).

Cyber provides a geometric increase in data transfer. In addition, the comprehensive collection provides the cyberattacker with the ability to distill the current situation, frame the desired effects, and perform cyber operations in order to produce the desired effects without traveling to the event location. The amount of data collected, and remediation cost due to a cyberattack, can be significant (Figure 1.1).

As shown in Figure 1.1, cyberattacks are increasing in both record count and subsequent remediation cost, and this is just in the commercial sector. Many private companies do not disclose that they have experienced a cyberattack due to the



*Cyber Operations: A Case Study Approach*, First Edition. Jerry M. Couretas.

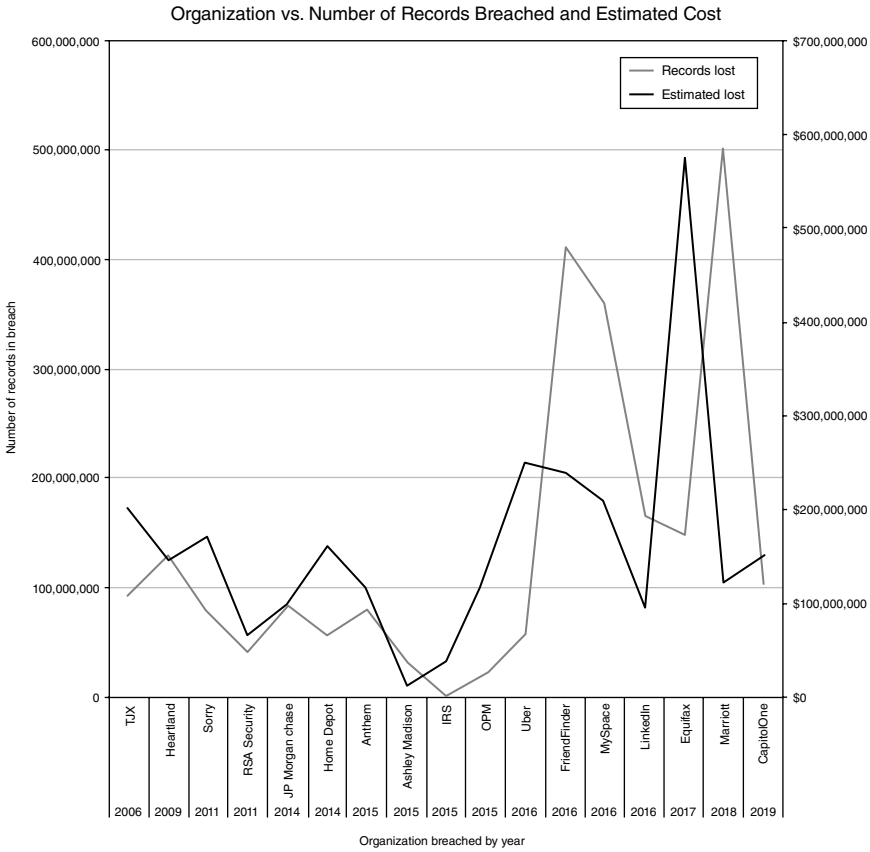


**Figure 1.1** Example Commercial Cyberattacks and Cost (2006–2019).

feared loss of customers. Government-operated, or provoked, cyberattacks can be an order of magnitude higher than the commercial attacks as found in Figure 1.1.

Government attacks are not so clearly spelled out, in terms of the number of records compromised or the remediation cost. In addition, government-operated attacks can be much larger. For example, the estimated $10 billion NotPetya attack in 2017 (Greenberg, 2019) brought global shipping to a standstill after infecting the back office planning and scheduling computers of Maersk, one of the largest goods transporters in the world. Computing the cost of cyber is an active area of research (Swallow, 2022).

The development of network-based computers also included a broad set of actors coming online. From media organizations to political campaigns to banks – every direct marketing organization interested in accessing a specific demographic developed an Internet presence. Political campaigns went online to bond with

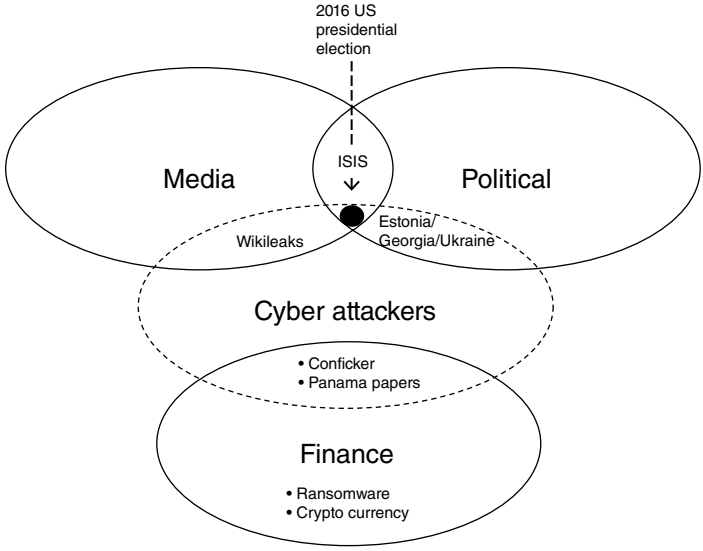


**Figure 1.2** Cyberattackers Operate in Multiple Domains.

their potential voters, banks went online to do business with their customers in real time, and people who just wanted to connect went online via social media. In addition, sales and marketing players use the Internet in order to increase their mind share through well-connected, lightly secured data, with cyberattackers (i.e., hackers) not far behind (Figure 1.2).

Media, political, and finance organizations shown in Figure 1.2 came online in order to expand their market reach and subsequently became common locations for cyberattack. One thing that each online organization has in common is a similar data access, management, and storage technique. Similar means and technical understanding are used to access, extract, and exploit the data of a media company, a political campaign, or a bank's key data stores. For example, cyberattackers used similar tools to access data from the U.S. State Department (i.e., cables exposed by Wikileaks) (Domscheit-Berg, 2011) or divulge data about shady offshore investments by global leaders (Panama Papers) (Bernstein, 2017). Each of these operations included collecting data from an "end point," and using that data to embarrass or steal from a target.

### 1.1.2 Hackers – Pre-Cyber Operations

Cyber operators span from hackers to nation-state operators. Hackers are often characterized as genuinely curious, computer-savvy folks who exceed their boundaries in tapping into private computer systems. White Hat hackers are known to tell the vulnerable system owner about what they found. Other

hackers might publicize private data, believing that "information wants to be free" (Levy, 2014).

Even before the rollout of personal computers, hacking was a game of wits between the hacker and the machine – a game of mental prowess. Early incarnations of the Internet (e.g., Arpanet) included hundreds, then thousands, of networked computers. It was only a matter of time before a determined hacker would test the limits of this new, networked, cyber world. The 1980s were therefore a time of early, but significant, activity in the cyber domain.

- The U.S. Government published the Computer Fraud and Abuse Act (Congress, 1986)
- The Morris Worm (1988), a rapidly replicating worm, was the first malware to shut down the ARPANET and cost hundreds of thousands of dollars to remediate
- "The Cuckoo's Egg," (Stoll, 2005), a book published in 1989, put a Soviet Russian KGB attack on U.S. government computers into story form – the goal of the KGB attack was to gain U.S. missile defense secrets

The popular movie "WarGames" (Badham, 1983) raised awareness about the dangers of computers and led to policymakers writing the Computer Fraud and Abuse Act (Congress, 1986). It was only a few years later, in 1988, that this law was used to prosecute Robert Tappan Morris for the damages that his "Morris Worm" perpetrated on the early Internet.

Due to the government's use of the pre-Internet to connect government and university computers, one of the first documented cyber operations included the KGB experimenting with the use of West German hackers to steal information on the U.S. Star Wars missile defense system in the 1980s. This occurred just before the breakup of the Soviet Union and subsequent government turmoil that delayed Russian use of cyber for espionage and information operations for approximately a decade.

In terms of technical development, Judge Greene broke up the AT&T telecommunications monopoly in 1984 (PINHEIRO, 1987). This ruling opened up the information technology market space in unforeseen ways, leading to the rich cyberspace landscape that we now have. The 1980s were also the years when Microsoft (1986) and Cisco (1990) went public, providing the computing and connectivity that dominates cyber terrain to this day.

At the same time that personal computers and networking were rapidly changing, the geopolitical order was put in flux due to the fall of the Soviet Union (1991) and the rapid changes in the military/political landscape. Russia started working its way toward a non-Soviet system and client states (e.g., Iraq) lost their superpower sponsorship.

Within a decade, during the late 1990s, Russian cyber operators were found hacking U.S. Air Force sites via Operation Moonlight Maze, pilfering

approximately 5.5 GB of documents (Kaplan, 2017). It was also around the end of the 20th century that Patriotic Hackers made their debut, becoming famous for defacing the White House website to protest the crash of one of their fighters harassing a U.S. EP-3 spy plane in the South China Sea (2000).

It was a few years later, in 2006, that Wikileaks came on the scene, using the Internet to expose offshore money laundering capers by foreign dignitaries, even causing Sigmundur Davíð Gunnlaugsson, President of Iceland, to abdicate over revelations in the Panama Papers (Bernstein, 2017).

Al Qaeda in Iraq (AQI) also debuted in the 2004–2005 time frame, using cyberspace to recruit, move money, and perform command and control. AQI's use of the web continued as the organizations morphed into the Islamic State of Iraq and Syria (ISIS) only to emerge from cyberspace as a military organization in 2011 and acquire a physical capitol in Raqaa, Syria, by 2014.

At the same time that ISIS and other players were sharpening their operational web techniques, Russia developed its cyber playbook by using Ukraine as a cyber-test bed (Greenberg, 2019). Russia conducted technical cyberattacks on power systems, banks, and tax authorities (i.e., NotPetya resulted in $10 billion in damage (Greenberg, 2019)). In addition, Russia mixed these technical cyberattacks with kinetic force to challenge governments in Georgia (2008) and Ukraine (≥2014). Russia also transitioned traditional active measures to the cyber domain in order to manipulate elections in the United States (2016 U.S. Presidential Election) (Mueller, 2019) and Europe (Cyware, 2021). Russia's use of cyber therefore goes above "the line" of non-kinetic conflict defined in Joint Doctrine Note 1–19, "Competition Continuum" (Joint Chiefs of Staff, 2019)(Figure 1.3).

As shown in Figure 1.3, cyber operations are generally "below the line." However, as cyber increasingly finds tactical applications, "above the line" actions have the potential to become more common for military/intelligence applications.

### 1.1.3 Cyber and Counter-Terror/Insurgency

Other examples of cyber operations include the ISIS using social media messaging to recruit, fund, and coordinate attacks. This included combining operations in ISIS' media and political domains in order to project a fundamentalist image and advertise battlefield successes during their development and operational stages, resulting in a 10 million person proto-state with a capitol in Raqaa, Syria, and a land mass that covered the size of Britain (Fox, 2019).

The development of Al Qaeda, AQI, and ISIS cyber operations coincided with the counter-terror (CT) and counter-insurgency (COIN) missions that spanned the first decades of the 21st century. As CT and COIN operations developed, the use of cyber to support tactical coalition operations rapidly expanded during counter-insurgency campaigns in Afghanistan and Iraq.

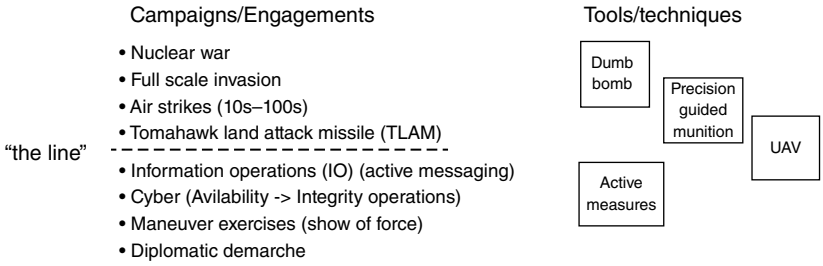


**Figure 1.3** Kinetic/Non-Kinetic Line of Hostility. *Source:* Adapted from Joint Chiefs of Staff, 2019.

While the use of the Internet by 9/11 attackers was a wake-up call, it was not until Coalition Operations in Afghanistan and Iraq, CT missions that morphed into COIN operations, that all source analysis started leveraging cyber in the form of social network analysis (SNA). For example, the overall theme of "Attack the Network" (AtN) (U.S. Joint Forces Command, 2011) required human targeting that included capturing leadership elements of adversary organizations on an unprecedented scale (Figure 1.4).

As shown in Figure 1.4, SNA is used to understand the composition and command structure of a given terror cell in order to identify cell members. Some of this membership/relationship information may be available via cyber, providing counter-IED/insurgency analysts with a tool for reducing the threat to coalition forces.

More specifically, counter-improvised explosive device (C-IED) operations used all source analysis in order to provide some of the beginnings of cyber analysis

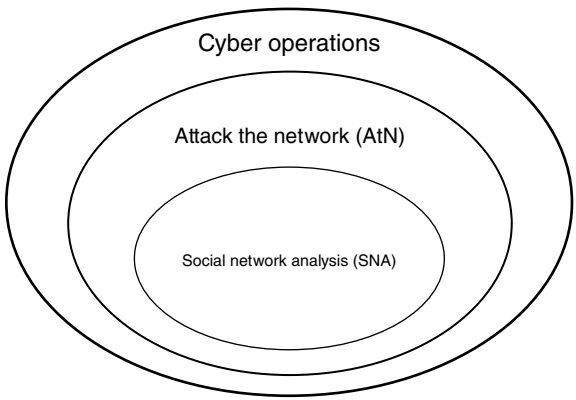


**Figure 1.4** Tactical Cyber Operations – Social Network Analysis (SNA) and Attack the Network (AtN).

and targeting. The employment of AtN and SNA techniques and technologies, therefore, developed into a solution to find and target these key individuals via their e-mail, social media, and communications traffic.

## 1.2 Early Internet and Cyber Operations

The importance of command and control (C2) in military operations inspired the idea of providing a network that could withstand a nuclear war. This resilient network eventually became the Internet (RAND). The Internet, provided to the public at the end of the Cold War, gave the world the ability to communicate globally, post information on newly pioneered websites, and search this information, for free. This was an incredible gift to a pre-Internet world that paid high rates for long-distance telephone calls and information searches that required a trip to the library.

A decade or so later, in the early 2000s, Chinese patriotic hacktivists were defacing the White House website as a means to protest the crash of a People's Liberation Army (PLA) jet, in the South China Sea, that was harassing a U.S. Navy EP-3 surveillance aircraft (2001) (Elisabeth Rosenthal, 2001). These were early signs that the Internet was being used by foreign actors to perform cyber operations. Then, in the aftermath of the 9/11 attacks (2001), the revelation that al Qaeda was using the Internet to communicate and transfer funds ended the Internet's age of innocence, with terrorists using the Internet for command and control (9/11 Commission, 2004).

The use of the Internet by Al Qaeda for e-mail communications/coordination, and website postings to disseminate their message, initially surprised counter-terror analysts. While "Network Centric Warfare" was still seen as a next-generation technical capability in the West, the employment of social media for tactical effect was already a developing tactic on the part of terror and IED networks in Iraq and Afghanistan (Schachtman, 2007).

### 1.2.1 Maturing of Cyber Operations – ISIS and Russia

Growing terror organizations' use of the web to publicize their activities, to attract funding, and to mobilize recruits created a new, cyber, domain of terror operations. Al Qaeda, then AQI, ISIL, and finally ISIS, refined their web presence, broadcasting many of their attacks in real time on Twitter (e.g., Capture of Mosul (2014)) (Emerson T. Brooking and Singer, 2016). ISIS effectively expanded from proselytization and funding operations to live messaging of kinetic attacks. ISIS also developed an ability to manufacture crowds on social media (Diresta, 2018), providing an implied substance, via the number of observable followers, that made them seem much larger than they were actually.

Terrorist organizations increased their coordination and media skills in conjunction with the growth of social media. Social media was just beginning during the AQI period (2004–2006). Facebook, for example, the main social media application for connecting people to long-lost classmates, friends, and relatives, debuted in 2004. Similarly, Twitter, the social media app for sending quick messages, pictures, and videos dates back to 2006.

The year 2006 was also the year that AQI remnants were defeated in Western Iraq's Al Anbar province via the U.S. Marine counter-insurgency program (Russell, 2010). This success inspired the U.S. Army's 2007 Surge, including the infusion of thousands of U.S. and Coalition troops into Eastern Iraq. The goal of the 2007 Surge was to isolate and defeat AQI and other groups, causing many of the insurgents to now conduct their propaganda, finance, and recruiting exclusively in cyberspace. This resulted in the remnants of the AQI guerilla network retreating to cyberspace, only to emerge as ISIS.

### 1.2.2 ISIS Cyber Operations

In the 2010–2011 time frame, the same time that the post-AQI organization was regrouping on the Internet, Wikileaks released a batch of U.S. Government "cables" that provided an insider's view of what U.S. diplomats thought of their peers across the world. These documents included an unflattering picture of Tunisia's ruling family, resulting in civil unrest and an eventual overturning of the government (Dickinson, 2011).

Starting in Tunisia, these mass protests spread across North Africa, with the governments of Egypt and Libya soon being overturned, as well. Called the Arab Spring (Rodenbeck, 2013), much of the reporting and coordination was performed on social media (e.g., Facebook, Twitter), showing the value of these platforms to target niche populations and messages for effect. The Arab Spring therefore became a cyber means to channel protestor frustration and overturn a Government locally, with International participation via online supporters and Internet-based social media technology (i.e., Facebook and Twitter). The Arab Spring also used social media to provide an alternative means to enfranchise both resident and nonresident (e.g., diaspora) "voters," in order to select candidate leaders and provide the messaging required to fuel protests, rallies, and demonstrations. These movements used social media to coordinate rallies and remove the existing government structure, leaving a power vacuum to be filled by more organized, and less liberal, politico-religious factions.

While the Arab Spring was overturning governments in North Africa, protests broke out in Syria, with a similar intent of overturning the Syrian government. Syrian government forces, however, fought back violently, resulting in a civil war that left large areas of the country effectively ungoverned. One of these

geographical security vacuums was filled by ISIS, emerging in January 2014, with a physical capitol in Raqaa, Syria, and near continuous social media operations. This was on the heels of Facebook's 2012 initial public offering (IPO) (Weidner, 2013) of their stock, and nearly coincided with Twitter's 2013 IPO (July 11, 2013) (Gabbatt, 2013).

### 1.2.3 Russian Cyber Operations

While social media was being used as a channel for antiregime protests and coordination in the North African Maghreb and Syria, Facebook was also being used to channel political angst in Russia. For example, the Snow Revolution (2011–2013) had up to 85,000 protestors showing up in Moscow's Bolotnaya Square to protest election results on December 10, 2011 (Ioffe, 2011). The power of social media was quickly recognized, with the Russian people starting to show their political Internet presence via Facebook accounts and tweets.

In reaction to the Snow Revolution, the Putin regime became aware of the power of social media. One action coming out of the Snow Revolution was for Putin's friend, Ilya Prigozhin[1], "Putin's Chef," to start the Internet Research Agency (IRA), in 2014. Among the IRA's tasks was to develop counter-messaging for adversaries to the Putin regime. As shown in Figure 1.5, the 2009–2018 timeline describes how the IRA provided a blitz of tweets against Ukraine during key events that include the Crimean invasion, the Internet response to the downing of Malaysian airliner MH-17, and the angry response to the 2014 Ukrainian elections.

The graph in Figure 1.5 shows the number of IRA-linked accounts created per day, overlaid with the number of tweets referencing Ukraine. The IRA was therefore developing additional accounts in conjunction with its message dissemination, adding an implied substance, via the size/scope of followers, in combination with the messaging. This is similar to what was observed in ISIS operations through the artificial construction of a movement via false accounts, manufactured personas, and super users "liking" content to provide implied validity.

Both Russia and ISIS showed a scaling up of followers, either from other countries/regions (ISIS) or completely virtual (Russia), in order to increase the online credibility of their messaging. And, while ISIS remained focused on political messaging and military exploits, Russia quickly shifted its cyber operations/propaganda between Ukrainian election results to counter-messaging on the reporting on Russian troops' shooting down of a civilian

1 Mr. Prigozhin is also famous for the June 23, 2023 "mutiny" against Russian Federation troops, resulting in him moving to Belarus with his Wagner Group private army. Mr. Prigozhin died in an airplane crash on August 23, 2023.

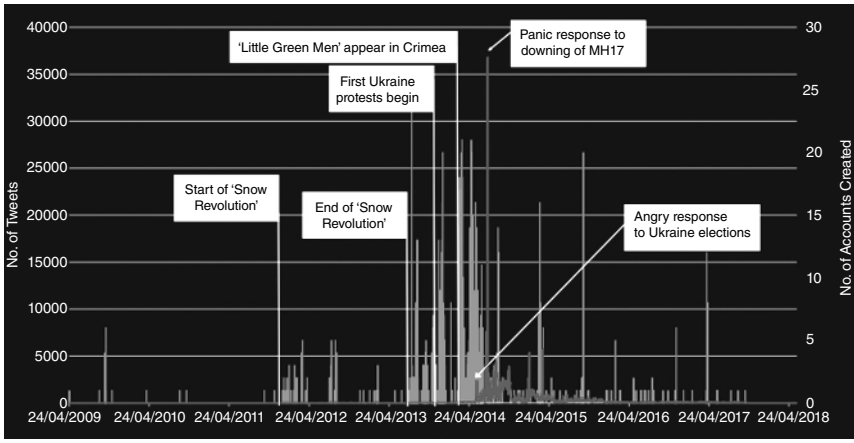


**Figure 1.5** Graph of tweets regarding Ukraine over time. *Source:* Cardiff Crime and Security Research Institute, 2019/Cardiff Crime and Security Research Institute.

aircraft (Bellingcat, 2015), to whitewashing its 2014 invasion of the Crimea. In short order, Russia showed the agility of its cyber operations to expand both the scale and scope of Internet messaging over a broad range of issues in order to promote the regime's objectives.

The longer-term response to the Snow Revolution included the Russian Federation's scaling up of online political operations. For example, the IRA set up a large number of new accounts in 2014 in order to target elections in Ukraine (Figure 1.5). In addition, these new accounts contributed to a campaign of increased scale and intensity surrounding the annexation of Crimea and the shooting down of Malaysia Airlines flight MH-17. This was also when Russia first turned off Ukraine's power with Industroyer malware (Slowik, 2019), duplicating their physical shutdown of Ukrainian gas pipelines in the 1990s (Smolansky, 1995).

## 1.3 Cyber Operations' Stage Descriptions

Long before the Russian use of cyber to bring active measures into the 21st century, the Internet was used by Al Qaeda and AQI to manage media, communications, recruiting, and money (Economist, 2007). Initial Al Qaeda use of the Internet was primarily the action of hackers. These initial Al Qaeda cyber operations were the first actions in what will be shown to be a three-staged progression of cyber tactics that range from the late 1990s to the present, and scale from early ideological hacking to current nation-state operations.

### 1.3.1 Stage I (late 1990s—~2010)(Community Development)

One of Al Qaeda's first reported webmasters, Younis Tsoulis (aka Irhabi007), managed money, recruiting, and website content from an apartment in London's West End during the early 2000s (Economist, 2007). Irhabi007 was followed by Anwar al-Awlaki, who provided direct inspiration for multiple attacks, several inside the United States, including Fort Dix (New Jersey) (2007), the Little Rock (Arkansas) military recruitment center (2009), and Fort Hood (Texas) (2009).

### 1.3.2 Stage II (~2010—~2015)(Tactical)

Following Anwar al Awlaki was Junaid Hussain (aka TriCk), who was already in trouble for hacking the phone of former British Prime Minister Tony Blair's chief aid, and publishing the downloaded information on the web, before joining ISIS. Hussain became the ISIS webmaster and was said to be in direct contact with the pro-ISIS players in the Garland, Texas, attack (2015). In addition, the ISIS that Hussain supported coordinated both the 2015 Paris nightclub attack (131 dead) and the 2016 Orlando nightclub attack (49 dead). Junaid Hussain, originally a simple hacker, proved to be more lethal by coordinating ISIS-inspired attacks. Stage II cyber operators therefore graduated from simple support to a command and control (C2) role.

### 1.3.3 Stage III (~2015 to present)(Tactical and Strategic)

The Stage II innovation of using cyber as a C2 method to guide operations was scaled up during Stage III. While terrorists were providing example Internet-based kinetic effects in the United States during Stage II, Russia used cyber to support military operations (from simple denial of service (DoS) operations to cyber-based active measures, e.g., 2007 Estonia, 2008 Georgia), shaping their campaigns through information operations. By 2014 Russia entered Stage III through the use of cyber operations to achieve strategic effects via election tampering, first documented in Ukraine (Figure 1.5), and then used in the 2016 U.S. Presidential election (Mueller, 2019).

The progressive development of cyber operations into what we are calling Stage III (Table 1.1), active election interference, looks a lot like traditional active measures, practiced extensively by the Soviet Union during the Cold War. An "active measure" is a term used for the political warfare actions conducted by the Soviet and Russian security services to influence the course of world events (Ewing, 2018). The goal of an active measure is to shape relationships to Soviet, now Russian, advantage, should an actual war break out. In addition, the term active measure is also used to describe the collecting of

**Table 1.1** Example Stages of Internet Use for Coordination, C2, and Social Media Weaponization.

| Cyber Operational Stage | Operator | Time Period | Description |
|---|---|---|---|
| Stage I | Younis Tsoulis (aka Irhabi007) | Early 2000s | Younis Tsoulis, a 22-year-old from London's West End, was the online webmaster for Al Qaeda (Economist, 2007) |
| | Anwar al-Awlaki | Late 2000s | Was in direct contact with perpetrators for<br>• 2007 Fort Dix Shooting<br>• 2009 Little Rock Recruiting Office Shooting<br>• 2009 Nidal Hasan attack at Fort Hood (killed 12, wounded 32)<br>• 2010 Times Square (New York City) bomber (failed) |
| Stage II | Junaid Hussain (aka TriCk) | Early 2010s | • 2011 Hacked British Prime Minister's (i.e., Tony Blair) personal assistant and published on the web<br>• Principal of TeaMp0isoN, executing Guerilla Warfare via the web<br>• Key ISIS cyberattacker<br>• 2015 In contact with Garland, Texas, physical attackers |
| Stage III | | Mid-2010s | • 2013 ISIS maintains a physical base in Raqaa, Syria<br>• 2015 ISIS responsible for coordinating 7 perpetrators for the November 2015 Paris attacks, initiated by 3 suicide bombers and resulting in the death of 131 victims and 413 critically injured<br>• 2016 ISIS-inspired Omar Mateen in the killing of 49 people in a mass shooting in Orlando, FL, USA |
| | Guccifer2.0 | | • Social media campaigns including over 10 million tweets in the 2016 U.S. Presidential Election (Cleary, 2019)<br>• Organized dozens of violent rallies in the United States between violent factions (Mueller, 2019)<br>• Used cyber to attack voting machines in several U.S. states with unclear objectives (e.g., disruption and influence outcome) (Pegues, 2018) |
| | Ransomware Groups (multiple) | Late 2010s | • Ransomware as a Service (RaaS)<br>– 2021 Colonial Pipeline and JBS Foods |

information and then the framing of that information to the information operator's advantage. While well known for almost 100 years (Popken, 2018), Russian active measures recently moved to the Internet in the form of information operations. The gradual maturing of cyber operations from hacking to providing strategic effects is provided in Table 1.1.

As shown in Table 1.1, while ISIS developed into a Stage III cyber operational actor out of its combined battlefield successes and persistent web presence, Russia's main intelligence agency, the GRU, built on ISIS' empirically proven web techniques and used similar social media tactics to participate in the 2016 U.S. presidential election. In addition, Russia's Internet Research Agency (IRA), formally a news organization, provided a steady stream of news and opinions (i.e., an estimated 10 million tweets (Cleary, 2019)), leading up to the 2016 U.S. Presidential Election. This includes the organization of dozens of issue-based rallies within the United States (Mueller, 2019), some of them turning violent (e.g., Garland Texas (2015), Charlottesville, Virginia (2017)).

The progression of cyber operations in Table 1.1 includes a timeline of the weaponization of social media from a simple tool for connecting friends and family, to a safe haven for terrorists, to a tool that is used to provide strategic economic and political effects. A quick look at this rapid progression of social media from hobby to weapon is provided in Figure 1.6.

As shown in Figure 1.6, Al Qaeda, AQI, and the ISIS were early users of social media for recruitment and C2. AQI was a Salafi Jihadist terrorist organization local to Iraq, loyal to the broader al Qaeda organization, led by Abu Musab Al Zarqawi. AQI was active from approximately 2004 to 2006, the time of Zarqawi's death (Burns, 2006). AQI also served as one of the initial anticoalition insurgent organizations in Iraq. For example, Abu Bakr al-Baghdadi, the ISIS leader from 2010 to 2019, served in AQI (The Wilson Center, 2019). ISIS therefore drew several lessons learned from AQI, including web-based communications.

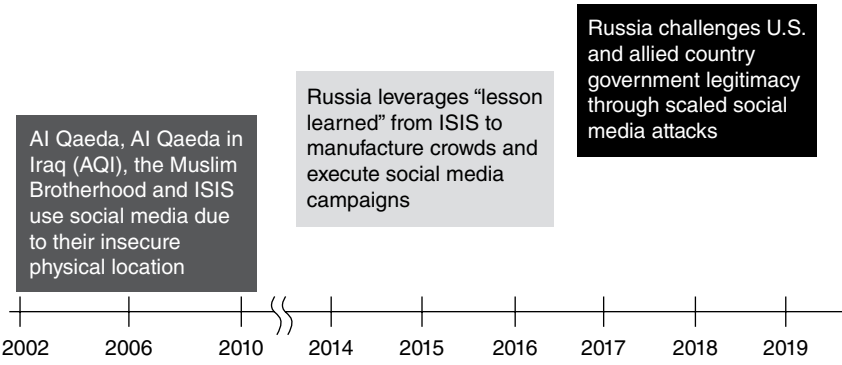


**Figure 1.6** Weaponized Social Media Timeline.

Russian cyber operations generalized on ISIS' proven social media successes in order to restore their ability to provide political effects through cyber-based active measures. For example, Russian cyber operations started with denial (2007 Estonia), gradually incorporated active measures (2008 Georgia, 2014 Crimea), while at the same time dabbling with operational technology surveillance (HAVEX malware (2014) in the United States and destruction (Industroyer (Ukraine 2014)) in Ukraine. Russia continued developing its active measures in cyber, using (1) the IRA to participate in the 2016 U.S. Presidential Election and (2) the Ghostwriter campaign to tamper with Western European election results (Cimpanu, 2021). More recently, the IRA's sister organization, the Wagner Group, has been shown to use ISIS recruitment techniques to provide additional manpower to the Russian war in Ukraine (Temple-Raston, 2023).

## 1.4 Cyber Operations Wrap-up

As shown in Figure 1.6, initial cyber operations in the information domain graduated to a physical presence in the case of both ISIS and Russia. And, while strategic communications are a recognized element of any military campaign, cyber adds a speed and scale unprecedented by print media. Similarly, we reviewed the evolution of cyber operations in Table 1.1, from hackers to professional intelligence services, that provide the social media presence and messaging that have become modern-day cyber effects.

The use of cyber for traditional espionage and information operations occurred over three stages (Section 1.3). Stage I, hacking and early coordination, spanned from the first networking of computers until approximately 2010. Stage I accelerated its development with the introduction of social media and the rollout of smartphones, culminating in the protestor coordination that formed the Arab Spring.

With the Internet as a proven medium for community organizing, Stage II included the command and control (C2) of tactical operations, including the control of terrorist attacks. The mass rollout of key social media channels (e.g., Facebook and Twitter), along with the emergence of ISIS from the web into a physical presence, were the key features of Stage II.

The Islamic State's cyber "occultation," starting with the 2006 defeat of AQI, had them emerging as ISIL in 2011, and a state (ISIS) with the capture of Raqaa, Syria, by 2014. This was a novel development that used new social media techniques. Supporters could now help ISIS from afar by manufacturing crowds and "liking" ISIS content in order to get it to the top of social media feeds. ISIS's social media techniques paid off. ISIS challenged the Iraqi government with a potential march on Baghdad in August 2014 (Freeman Spogli Institute, 2021). In addition,

ISIS's social media techniques were keenly observed by Russia, with the IRA using personas and Facebook messaging to participate in multiple elections, including the 2016 U.S. Presidential Election.

Stage III was the nation-state assimilation (Russia) of proven ISIS tactics for strategic effect. Elections in the Ukraine and the United States are two examples of where Russia used cyber effects in an attempt to influence election outcomes. For example, starting around the run-up to the 2016 U.S. Presidential Election, Russia showed how a web-based actor (e.g., IRA, Guccifer 2.0) could induce political/kinetic effects in another country through the organization of rallies between extremists on opposing sides of a political spectrum. The IRA and Guccifer 2.0 were the perpetrators identified in the investigation of over 100 violent rallies in the days leading up to the 2016 U.S. Presidential Election (Mueller, 2019).

By 2015, a 20-year-old Internet had matured through three stages of operational development in becoming a mechanism for 21st-century political manipulation; a means to achieve strategic effects. Cyberspace had also become a breeding ground for radical operators to coordinate recruits and financing, with ISIS proving that an organization could take refuge, maneuver, and emerge from cyberspace as a political entity with a physical presence.

## Bibliography

9/11 Commission. (2004). *The 9/11 Commission Report*. Retrieved 8 4, 2019, from https://www.9-11commission.gov/report/911Report.pdf.

Badham, J. (Director). (1983). *WarGames* [Motion Picture].

Bellingcat. (2015). *MH17 – The Open Source Evidence*. Retrieved from Bellingcat: https://www.bellingcat.com/app/uploads/2015/10/MH17-The-Open-Source-Evidence-EN.pdf.

Bernstein, J. (2017). *Secrecy World – Inside the Panama Papers Investigation of Illicit Money Networks and the Global Elite*. New York, NY, USA: Henry Holt and Company.

Burns, J. F. (2006). *U.S. Strike Hits Insurgent at Safehouse*. Retrieved 2 20, 2022, from New York Times: https://www.nytimes.com/2006/06/08/world/middleeast/08cnd-iraq.html.

Cardiff Crime and Security Research Institute. (2019). *THE Internet Research Agency in Europe 2014-2016*. Retrieved 2 26, 2022, from Cardiff Crime and Security Research Institute: https://www.cardiff.ac.uk/__data/assets/pdf_file/0004/1490548/CSRI-IRA-Report-Final.pdf.

Cimpanu, C. (2021). *EU Formally Blames Russia for GhostWriter Influence Operation*. Retrieved from The Record: https://therecord.media/eu-formally-blames-russia-for-ghostwriter-hack-and-influence-operation.

Cleary, G. (2019). *Twitterbots: Anatomy of a Propaganda Campaign*. Retrieved 7 6, 2019, from Symantec: https://www.symantec.com/blogs/threat-intelligence/twitterbots-propaganda-disinformation.

Congress. (1986). *H.R.4718 – Computer Fraud and Abuse Act of 1986*. Retrieved from 99th Congress: https://www.congress.gov/bill/99th-congress/house-bill/4718.

Crumpton, H.A. (2012). *The Art of Intelligence: Lessons from a Life in the CIA's Clandestine Service*. Penguin.

Cyware. (2021). *Ghostwriter: A Russia-Linked Influence Campaign*. Retrieved 9 1, 2021, from Cyware: https://cyware.com/news/ghostwriter-a-russia-linked-influence-campaign-51f90ed0.

Dickinson, E. (2011). *The First WikiLeaks Revolution?* Retrieved 5 15, 2023, from Foreign Policy: https://foreignpolicy.com/2011/01/13/the-first-wikileaks-revolution/.

Diresta, R. (2018). *How ISIS and Russia Won Friends and Manufactured Crowds*. Retrieved 7 7, 2019, from Wired: https://www.wired.com/story/isis-russia-manufacture-crowds/.

Domscheit-Berg, D. (2011). *Inside Wikileaks – My Time with Julian Assange at the World's Most Dangerous Website*. New York: Crown.

Economist. (2007). *A World Wide Web of Terror*. Retrieved 8 11, 2019, from Economist: https://www.economist.com/briefing/2007/07/12/a-world-wide-web-of-terror.

Elisabeth Rosenthal, D. E. (2001). *U.S. Plane in China After it Collides with Chinese Jet*. New York Times.

Emerson T. Brooking, Singer, P.W. (2016). *WAR GOES VIRAL – How Social Media is Being Weaponized Across the World*. Retrieved 2 27, 2022, from The Atlantic: https://www.theatlantic.com/magazine/archive/2016/11/war-goes-viral/501125/.

Ewing, P. (2018). *The Russia Investigations: What You Need To Know About Russian 'Active Measures'*. Retrieved from NPR: https://www.npr.org/2018/04/25/586099619/the-russia-investigations-what-you-need-to-know-about-russian-active-measures.

Fox, G. (2019). *ISIS Caliphate Defeated: A Timeline of the Terror Group's Brutal Project*. Retrieved 2 26, 2022, from Independent: https://www.independent.co.uk/news/world/middle-east/isis-timeline-caliphate-iraq-syria-territory-defeated-a8782351.html.

Freeman Spogli Institute. (2021). *The Islamic State*. Retrieved from Stanford Center for International Security and Cooperation: https://cisac.fsi.stanford.edu/mappingmilitants/profiles/islamic-state.

Gabbatt, A. (2013). *This Article is more than 8 Years Old Twitter IPO: Shares Begin Trading at $45.10 – Live Coverage*. Retrieved 2 20, 2022, from Guardian: https://www.theguardian.com/technology/2013/nov/07/twitter-ipo-public-stock-live-updates.

Greenberg, A. (2019). *Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers*. Doubleday.

Ioffe, J. (2011). *Julia Ioffe*. Retrieved 2 27, 2022, from New Yorker: https://www.newyorker.com/news/news-desk/snow-revolution.

Joint Chiefs of Staff. (2019). *Joint Doctrine Note 1–19 – Competition Continuum*. Retrieved 5 10, 2020, from Joint Chiefs of Staff.

Joint Staff. (2018). *Joint Publication 3–12 Cyberspace Operations*. Retrieved 9 16, 2019, from Joint Publications: https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf.

Kaplan, F. (2017). *Dark Territory: The Secret History of Cyber War*. New York: Simon & Schuster.

Levy, S. (2014). *Hackers at 30: "Hackers" and "Information Wants to Be Free"*. Retrieved 5 15, 2023, from Wired: https://www.wired.com/story/hackers-at-30-hackers-and-information-wants-to-be-free/.

Mandiant. (n.d.). *Advanced Persistent Threats (APTs)*. Retrieved 5 2, 2023, from Mandiant: https://www.mandiant.com/resources/insights/apt-groups.

Microsoft. (2022). *Ransomware as a Service: Understanding the Cybercrime Gig Economy and how to Protect Yourself*. Retrieved 11 15, 2022, from Microsoft Defender Threat Intelligence Microsoft Threat Intelligence Center (MSTIC): https://www.microsoft.com/en-us/security/blog/2022/05/09/ransomware-as-a-service-understanding-the-cybercrime-gig-economy-and-how-to-protect-yourself/#threat-actors-campaigns.

Mueller, R. (2019). *Report On The Investigation Into Russian Interference In The 2016 Presidential Election*. U.S. Department of Justice. Washington: U.S. Department of Justice.

Pegues, J. (2018). *Kompromat – How Russia Undermined American Democracy*. Amherst, NY: Prometheus.

Pinheiro, J. (1987). AT&T divestiture & the telecommunications market. *High Technology Law Journal 2* (2): 303–355.

Popken, B. (2018). *Factory of lies: Russia's disinformation playbook exposed*. Retrieved 3 22, 2020, from NBC News: https://www.nbcnews.com/business/consumer/factory-lies-russia-s-disinformation-playbook-exposed-n910316

RAND. (n.d.). *Paul Baran and the Origins of the Internet*. Retrieved 2 20, 2022, from RAND: https://www.rand.org/about/history/baran.html.

Rodenbeck, M. (2013). Special Report – The Arab Spring. *Economist*.

Russell, J. A. (2010). *Innovation in War: Counterinsurgency Operations in Anbar and Ninewa Provinces, Iraq, 2005–2007*. Retrieved 2 19, 2021, from Taylor and Francis: https://www.tandfonline.com/doi/full/10.1080/01402390.2010.489715.

Schachtman, N. (2007). *How Technology Almost Lost the War: In Iraq, the Critical Networks Are Social — Not Electronic*. Retrieved 5 13, 2023, from Wired: https://www.wired.com/2007/11/ff-futurewar/.

Slowik, J. (2019). *CRASHOVERRIDE: Reassessing the 2016 Ukraine Electric Power Event as a Protection-Focused Attack*. Retrieved 9 24, 2019, from DRAGOS: https://dragos.com/wp-content/uploads/CRASHOVERRIDE.pdf.

Smolansky, O. M. (1995). Ukraine's Quest for Independence: The Fuel Factor. *Europe-Asia Studies*, *47*(1), 67–90. Retrieved from https://www.jstor.org/stable/153194.

Stoll, C. (2005). *The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage*. Pocket Books.

Swallow, C. (2022). *Considering the Cost of Cyber Warfare: Advancing Cyber Warfare Analytics to Better Assess Tradeoffs in System Destruction Warfare*. Retrieved 12 14, 2022, from Journal of Defense Modeling and Simulation: https://journals.sagepub.com/doi/abs/10.1177/15485129221114354?journalCode=dmsa.

Temple-Raston, D. (2023). *Russia's Wagner Group Uses Recruitment Efforts Honed by ISIS*. Retrieved from TheWorld: https://theworld.org/media/2023-06-07/russias-wagner-group-uses-recruitment-efforts-honed-isis.

The Wilson Center. (2019). *Timeline: The Life and Death of Abu Bakr al Baghdadi*. Retrieved 2 20, 2022, from https://www.wilsoncenter.org/article/timeline-the-life-and-death-abu-bakr-al-baghdadi.

U.S. Joint Forces Command. (2011). *Commander's Handbook for Attack the Network*. Retrieved 8 4, 2019, from https://www.jcs.mil/Portals/36/Documents/Doctrine/pams_hands/atn_hbk.pdf.

Warner, M. (2017). Intelligence in Cyber – and Cyber in Intelligence. In: *Understanding Cyber Conflict – 14 Analogies* (ed. A.L.G. Perkovich), 265–272. Washington DC: Georgetown.

Weidner, D. (2013). *Facebook IPO Facts, Fiction and Flops*. Retrieved from Wall Street Journal.