How A Digital Footprint Provides A Criminal Foothold

By Dr. Georgianna Shea

Executive Summary

The threat to U.S. national security and economic prosperity from ransomware, cyber-enabled intellectual property theft, and malicious code inserted into key supply chains is rising. So too is the adversarial manipulation of American elections, America's cultural divides, and the broader fundamentals of American democracy.

Billions of dollars and some of the nation's brightest minds are working to shore up networks and infrastructure under attack. However, nearly all academic research on countering the effects of influence operations since the early 1970s has focused on fact-checking and other efforts to educate consumers so they do not fall victim to disinformation, according to a Harvard study.[1] Little research has focused on interventions that undermine or disable the disinformation operation and its enabling infrastructure.

FDD's Transformative Cyber Innovation Lab (TCIL) conducted a live-fire pilot demonstrating the similarities between offensive cyber operations and cyber-enabled influence operations. TCIL partnered with the Sports Information Sharing and Analysis Organization (ISAO)[2] and its primary sponsor, the nonprofit Cyber Resilience Institute,[3] to conduct the pilot. TCIL leveraged Sports-ISAO's open-source threat hunting and analysis capability during the 2022 Beijing Winter Olympics. The project identified the tactics, techniques, and procedures (TTPs) malicious actors use to create operational infrastructure to spread disinformation, commit fraud, and compromise systems.

After assessing the commonality in the operational digital footprint, this study offers recommendations to obstruct cyber and influence operations by identifying the dangerous loopholes in internet infrastructure that allow criminals to find safe haven.

Commonly Observed Tactics to Prepare the Battlefield

To operate in cyberspace, malicious and benign actors need infrastructure — the domains, domain name systems, virtual private servers, servers, and web services that make up the internet. To conduct malicious operations, actors illegally compromise existing infrastructure or legally buy, lease, or rent their infrastructure.

Gray Infrastructure

When legitimate owners of infrastructure turn a blind eye to questionable activity, the platform and services are known as "gray infrastructure."[4] While the provider may be legitimate, they may not take sufficient action to prevent abuse. The service providers may purposely configure their products to shield criminal activity from global law enforcement investigations or otherwise operate in jurisdictions with lax law enforcement.[5] For example, rogue cryptocurrency exchanges ignore the Digital Millennium Copyright Act (DMCA), and disreputable providers purposely do not collect or store client information.

1. Laura Courchesne, Julia Ilhardt, and Jacob N. Shapiro, "Review of social science research on the impact of countermeasures against influence operations," *Misinformation Review, Harvard Kennedy School*, September 13, 2021. (https://misinforeview.hks.harvard.edu/article/review-of-social-science-research-on-the-impact-of-countermeasures-against-influence-operations/)

2. Sports-ISAO is a membership organization of industry and academic stakeholders committed to the physical and cybersecurity of sporting events. See: https://sports-isao.org/

3. "About us," *The Cyber Resilience Institute*, accessed January 4, 2023. (https://www.cyberresilienceinstitute.org/about-us/)

4. Europol, "Internet Organised Crime Threat Assessment (IOCTA) 2021," 2021, page 18. (https://www.europol.europa.eu/publications-events/main-reports/internet-organised-crime-threat-assessment-iocta-2021)

5. Maria Konte, Roberto Perdisci, and Nick Feamster, "ASwatch: An AS Reputation System to Expose Bulletproof Hosting ASes," *SIGCOMM '15: Proceedings of the 2015 ACM Conference on Special Interest Group on Data Communication*, August 17, 2015. (https://dl.acm.org/doi/10.1145/2785956.2787494)

How A Digital Footprint Provides A Criminal Foothold

Sometimes, adversaries and criminals use gray infrastructure to deceive or trick potential victims into trusting the attackers' websites, emails, and other operational infrastructure. Yet globally, there is little to no regulation requiring domain name resellers and website certification authorities to validate the buyer's or provider's identity.[6]

Domain Name System (DNS) Abuse

A common obfuscation method to create illicit infrastructure that appears authentic is Domain Name System (DNS) abuse.[7] DNS abuse techniques include purchasing domain names that exploit typosquatting and domain parking. Typosquatting spoofs popular websites by using a misspelling of a legitimate domain. Domain parking involves creating a non-fully functional website on a domain as a staging platform. The site is disconnected from the rest of the domain and has no active content. Some domain owners will sell unused domain names to advertisers to use like a billboard, in exchange for a pay-per-click. Malicious actors, however, can also take advantage of popular unused domain names by using the parked domain to redirect the viewer to another site hosting malware. For example, if FDD did not own and secure all iterations of its URL, an attacker might create fdd.org/Olympics that reverted to a malicious staging site rather than a 404 page on FDD's website.

Certificate Authority Abuse

Certificate authority abuse is another method to deceive users. Digital certificates on websites demonstrate that a third party has validated and authenticated the site's ownership. However, not all certificate-issuing authorities validate the owners' identification during registration. To trick website visitors, malicious actors obtain digital certificates from less reputable certificate authorities requiring no verification. Even when customers provide no verification, website visitors will still see a lock icon to the left of a website address, leading visitors to believe the site is authentic and secure when it is not.

Fake Accounts

On social media, malicious actors create large volumes of fake accounts or hijack legitimate accounts using credentials compromised in breaches. The malicious actors use the accounts to amplify the activity of a primary account (base account) and steer visitors to the established enabling operational infrastructure created through gray infrastructure, DNS abuse, and certificate authority abuse.

As detailed in the following section, the FDD pilot results demonstrated that actors use these same TTPs to build operational infrastructure whether they plan to conduct espionage, launch an influence operation, extort money from victims, engage in cyber sabotage, or initiate other malicious operations.

Table 1: Common Tactics Detected in Observed Campaigns

	DNS Abuse	Gray Infrastructure	Certificate Authority Abuse
Disinformation Campaign	X (typosquatting)	X	X
Malware Campaign		X (ad fraud)	
Fraudulent Use of Media	X	X	X

6. Michael Hsieh, David Wu, and Doug Wood, "Is the Padlock on Your Browser Bar Giving You a False Sense of Security? How Trust is Managed (and Mismanaged) on the Internet," *Foundation for Defense of Democracies*, July 6, 2020. (https://www.fdd.org/analysis/2020/07/06/is-the-padlock-on-your-browser-bar-giving-you-a-false-sense-of-security/)

7. "Fronton: A Botnet for Creation, Command, and Control of Coordinated Inauthentic Behavior," *NISOS*, May 19, 2022. (https://www.nisos.com/blog/fronton-botnet-report/)

How A Digital Footprint Provides A Criminal Foothold

Pilot Description and Findings

Large-scale events attract opportunistic threat actors who prey on unsuspecting individuals. Criminals take advantage of fans who want to watch, communicate, and research information related to concerts, social events, and sporting events. The 2022 Beijing Olympics was of particular interest to a U.S. government client, which asked Sports-ISAO to use open-source intelligence to provide indications and warnings of malicious influence and offensive cyber operations surrounding the games.

First, the Sports-ISAO team worked with the U.S. government client to identify target topics for collection, known as priority intelligence requirements (PIRs). Rather than trying to track down every data point that might indicate suspicious activity, the PIRs included the disinformation themes that subject matter experts anticipated pro-Chinese Communist Party (CCP) actors would use to advance or amplify official party narratives and themes. These themes included CCP narratives around COVID-19 origins, Taiwan, and human rights as well as Russian government narratives about doping and its military build-up around Ukraine. The client was also interested in influence and offensive cyber operations targeting U.S. government personnel, sponsoring companies, Olympic participants, and fans.

After establishing the high-level PIRs, the team planned their discovery operations — the hunt — to identify observable activity within the scope of the PIRs. Sports-ISAO used two different hunt teams: the Cyber Observable Threat Hunters, which focused on the technical data, and the Social Media Hunt Team, which focused on the human relationships and interactions found on social media platforms. The small teams used established research techniques to gather and analyze technical data. Together, the two teams complemented each other's work to gain a complete picture of the activity, use of infrastructure, and influence operations techniques. The team discovered three significant types of campaigns — disinformation, malware, and fraudulent media use.[8]

TCIL was particularly interested in the similarities between the enabling infrastructure used in influence and cyber operations partly because of Sports-ISAO's prior findings during similar missions. For example, during previous global sporting events, Sports-ISAO had identified relationships between pop-up streaming services and malware-laden websites. These websites also impersonated popular sites as part of influence operations.

Sports-ISAO begins its research for major sporting events with a routine domain check. The group investigated the official domain beijing2022.cn to see what similar domain names were also registered. As a result, analysts discovered questionable websites established specifically for the games by financially motivated actors. Some sites contained ads for various products, redirects to other sites, and unauthorized streaming services.

Eleven domains within the ".cn" domain appear to have been registered by typosquatters, who trick the user into visiting a replica site that looks almost identical to the desired URL address.[9]

8. The following sections summarize the findings of the hunt reports. More information about the technical artifacts, methodology, and conclusions is available upon request.

9. "Domain Parking Program," *Bosis*, accessed January 4, 2023. (https://www.bodis.com/terms/domain-parking-program)

How A Digital Footprint Provides A Criminal Foothold

Table 2: Observed Websites with Typosquatting

URL	Typosquatting Technique	Explanation
Beijing2022.cn	***None***	***Correct URL address***
beijing2023.cn	Bitsquatting	A change in the value of the characters (changed value of 2022 to 2023, 2020, and 2026).
beijing2020.cn		
beijing2026.cn		
beij1ng2022.cn	Homoglyph	Replacing a character with one that resembles the correct character (replaced the letter i with the number 1).
beijing-2022.cn	Hyphenation	Adding a hyphen (added a hyphen between beijing and 2022).
beijiing2022.cn	Insertion	Adding extra characters (added extra i).
beijing202.cn	Omission	Removes characters (removed the number 2)
beijing222.cn		Removes characters (removed the number 0)
beiiing2022.cn	Replacement	Replaces characters (replace j with i)
beijing.2022.cn	Subdomain	Adds periods to the address (added a period between beijing and 2022, making it appear to be a subdomain).
beijing20.22.cn		Adds periods to the address (added a period between bejing20 and 22, making it appear to be a subdomain)

Disinformation Campaign Findings

Collecting on human rights PIR, the team honed in on the Chinese treatment of the Uyghurs and propaganda directed at young people. The teams began by leveraging news reports and social media, focusing particularly on two Twitter networks that the Media Forensics Hub at Clemson University had previously attributed to the People's Republic of China.[10] Media Forensics Lab observed many of the accounts involved in these networks were new, while others appeared to be compromised accounts from a 2014 hack repurposed to participate in propaganda.[11]

The first Twitter network consisted of accounts using the hashtag #GenocideGames, first created by protesters and dissidents to draw attention to China's human rights abuses. However, this pro-China influence network attempted to hijack this hashtag through "flooding." This is a common technique to control content, shape online conversations, or drown out opposing views.

For example, a typical Twitter post by a Chinese troll about the Xinjiang province may include a short video of a cotton field in Xinjiang and use the hashtags #humanrights, #cotton, #xinjiang, #forcedlabor, and #uyghur. However, users

10. Georgia Wells and Liza Lin, "Pro-China Twitter Accounts Flood Hashtag Critical of Beijing Winter Olympics," *The Wall Street Journal*, February 8, 2022. (https://www.wsj.com/articles/pro-china-twitter-accounts-flood-hashtag-critical-of-beijing-winter-olympics-11644343870)

11. Darren Linvill, Patrick Warren, Steven Sheffield, Jayson, Warren, Beau Brierre, Grant Cole, Jonathan Heijjer, Tyler Reich, Grant Saunders, and Jack Taylor, "Xinjiang Nylon: The anatomy of a coordinated inauthentic influence operation," *Media Forensics Hub, Clemson University*, December 2021. (https://www.clemson.edu/centers-institutes/watt/hub/documents/ci-xinjiang-influence-operation2021.html)

searching for conversations using these hashtags will more likely find content on farming than mistreatment of Uyghurs in Xinjiang.[12] Media Forensics Hub theorized the flooding campaign might also have been designed to trigger Twitter's anti-spam algorithms to remove tweets using the hashtag, including legitimate protesters' tweets.

Using simple Twitter searches based on the social media personas mentioned in a *Wall Street Journal* article about Media Forensics Hub's findings,[13] the team identified 25 base accounts and additional amplifier accounts. The team did not assess the total number of actual people, bots, or compromised accounts, but it concluded that many of the tweets were generated automatically.

While evaluating the campaign's effectiveness was beyond the scope of the hunt mission, the team concluded that the campaign was likely ineffective.

The second Twitter network consisted of more than 3,000 accounts, created recently with very few followers, sharing posts from state media accounts. After press reports highlighted the network,[14] Twitter removed hundreds of the accounts for violating the company's policies on manipulation and spam activity.[15]

Before this removal, a notable subset of the accounts had been reposting tweets from one account, Spicy Panda. At the time of the Winter Olympics, that account was less than a year old and featured an endearing panda logo with the description, "Shed light on the unspoken truth and offer sharp and spicy insights into the changing world." As of February 19, 2022, the account had 44,952 followers. Over the previous five months, it had sent an average of 6.38 tweets per day, 65 percent of which were in English and 34 percent were in Mandarin. Tweets were largely Sinocentric, praising China and its achievements while criticizing the United States and the West.

Pro-China tweets included benign pictures of kittens, photos of Chinese landscapes, and proud statements about Chinese culture. Tweets also praised China's purported achievements in poverty alleviation, innovative technology, 5G, space, green energy, COVID containment, law and order in Hong Kong, the Belt and Road Initiative, and all the medals won by Chinese athletes during the Olympics.

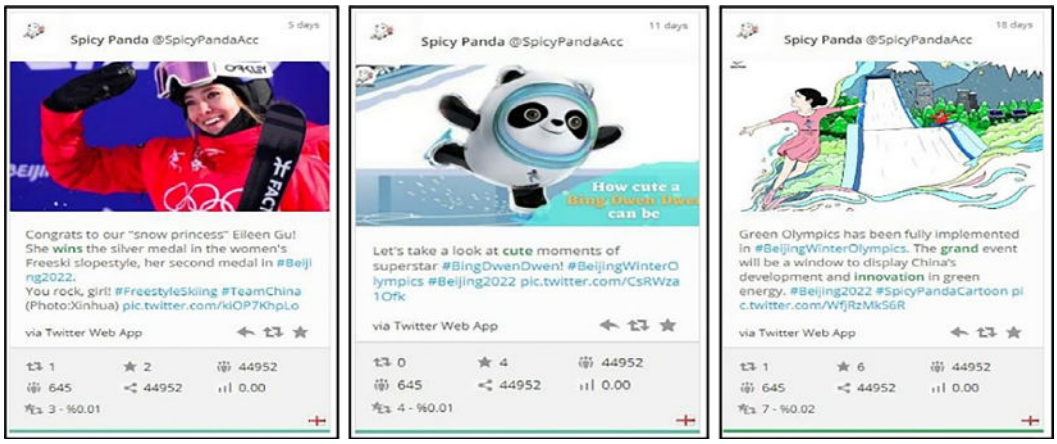


Figure 3: Pro-China tweets

12. Darren Linvill and Patrick Warren, "Understanding the Pro-China Propaganda and Disinformation Tool Set in Xinjiang," *Lawfare*, December 1, 2021. (https://www.lawfareblog.com/understanding-pro-china-propaganda-and-disinformation-tool-set-xinjiang)

13. Georgia Wells and Liza Lin, "Pro-China Twitter Accounts Flood Hashtag Critical of Beijing Winter Olympics," *The Wall Street Journal*, February 8, 2022. (https://www.wsj.com/articles/pro-china-twitter-accounts-flood-hashtag-critical-of-beijing-winter-olympics-11644343870)

14. Steven Lee Myers, Paul Mozur, and Jeff Kao, "Bots and Fake Accounts Push China's Vision of Winter Olympic Wonderland," *The New York Times* and *ProPublica*, February 18, 2022. (https://www.nytimes.com/2022/02/18/technology/china-olympics-propaganda.html)

15. Hannah Towey, "Twitter suspended hundreds of fake Chinese propaganda accounts that promoted the Beijing Olympics while glossing over human rights controversies," *Business Insider*, February 20, 2022. (https://www.businessinsider.com/twitter-suspends-hundreds-of-bots-posting-chinese-olympic-propaganda-2022-2)

How A Digital Footprint Provides A Criminal Foothold

Negative tweets included criticism of the U.S. president and the withdrawal from Afghanistan, discussions of racism in the United States, accusations that the West keeps Africa in poverty, allegations of attempted American sabotage of the Olympics, and alleged American disinformation about the Uyghur genocide in China. Overall, the negative tweets promoted the theme of a crumbling U.S. democracy.

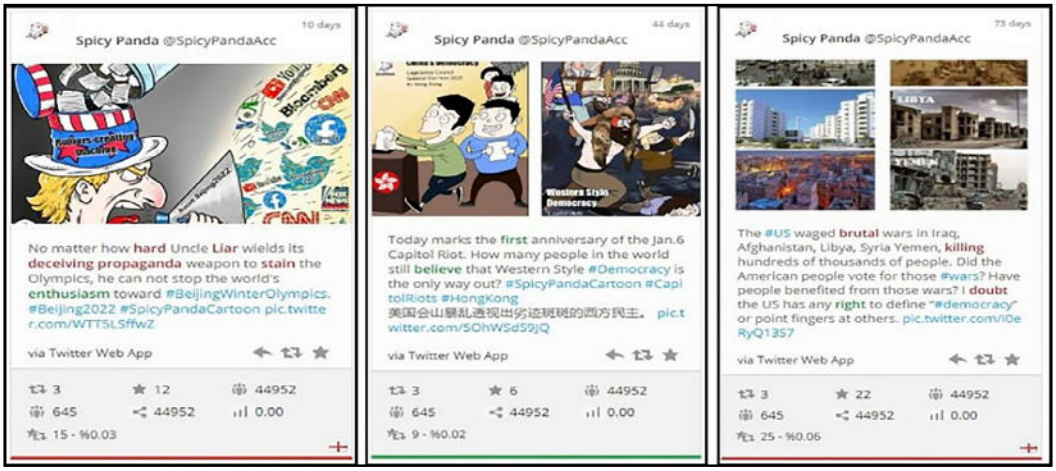


Figure 4: Negative U.S. tweets

After the Beijing Olympics, the account switched to the looming Ukraine war, parroting Russian propaganda and other pro-Putin content, including a February 23 video of China's government spokesperson, Hu Chunying, blaming the U.S. for the situation. At that point, Twitter permanently suspended Spicy Panda for violating its policies.[16]

A professor at the Media Forensics Lab called Spicy Panda "one of the best quality Chinese propaganda accounts I've ever seen."[17] The hunt team compared Spicy Panda's large numbers of tweets, retweets, views, and impressions to those of known Chinese domestic and foreign influencers and official CCP spokespersons. Based on this comparison, the hunt team concluded that Spicy Panda was far less effective than known influencers and official spokespersons. However, the team warned that both observed disinformation operations indicated that the Chinese Communist Party was beginning to engage more with western audiences. "The scale of these operations means we need to pay attention," warned Sports-ISAO.

Malware Campaign Findings

While investigating information related to the malware PIR and fraudulent activity directed toward fans, the teams uncovered an extensive cyber campaign on an ad network operating from a legitimate China-based e-commerce company. The hunt team discovered this campaign because the e-commerce website sells sports memorabilia and is one of the top three e-commerce websites in China and Southeast Asia. Victims of this campaign were likely Chinese-speaking fans in China and Southeast Asia.

The team believes this was part of an ongoing campaign using Hiddad malware targeting Android mobile devices and computers using Microsoft operating systems. Hiddad malware pushes as many ads as possible to end-users to make money by registering impressions and views, taking advantage of pricing differences among automated advertising brokerages.

16. @drewharwell, *Twitter*, February 25, 2022. (https://twitter.com/drewharwell/status/1497229789475786753)

17. Andy Kroll, "China's Propaganda Machine Gears Up for Putin — and Blames America for the Invasion," *Rolling Stone*, March 2, 2022. (https://www.rollingstone.com/politics/politics-features/russia-china-ukraine-propaganda-invasion-ccp-1315024/)

How A Digital Footprint Provides A Criminal Foothold

Like with the disinformation campaign, the team observed various social media accounts steering readers to websites with characteristics of DNS and certificate authority abuses featuring malicious software. In this campaign, the adversary inserted the malware on the endpoint devices when victims visited websites advertised on Twitter.

Hundreds of new domain names also resolving to the same infected website were registered throughout the Beijing Olympics. Most of the staging activity occurred before the start of the games. The research team found over 300 domains registered on the day of the Beijing Olympics closing ceremony alone. Many sites affiliated with the infected website had newly registered certificates. Some were phishing sites used to spread malware.

The team also found the malware "ryuk[.]exe." Ryuk is Russian-based ransomware, but since it is available for purchase, the team could not determine if Russian cyber actors were involved. The Sports-ISAO team assessed the party responsible for the malware cluster was managed by a well-funded criminal enterprise opportunistically exploiting multiple vulnerabilities in the advertising ecosystems. This includes vulnerabilities in end-user devices (computers, iPads, mobile devices), ad brokerage algorithms, and network vulnerabilities. Evidence from this investigation indicates that malicious actors may have infected unsuspecting victims to install spyware and harvest their user credentials.

Fraudulent Use of Media Campaign Findings

According to sports marketing company Infront, the potential damage worldwide from sports piracy is $12.5 billion annually.[18] Fraudulent live streaming presents both copyright and cybersecurity challenges. Larger fraudulent video streamers build sustainable businesses through subscriptions and digital advertising, portraying themselves as defenders of the consumer against "evil corporations" who charge high fees and make it cost-prohibitive for fans to access the content. These streamers violate copyright law but do not harm consumers. Other providers, especially smaller ones, use phishing, credit card fraud, and other malware to make a profit.

The team discovered two malicious networks illegally streaming the Olympics when investigating free streaming sites that might contain malware or credit card and ad fraud. The social media hunt team also found fraudulent activity connected to a network active during the Tokyo Olympics and other prior sporting events. The cyber hunt team discovered a new fraud network.

The social media team scoured Twitter to find free streaming services that offered Olympics coverage. In addition to terms such as "free streaming," the team included event-specific hashtags such as:

#OlympicGames
#Beijing2022
#Olympics2022
#WinterOlympics
#Olympics
#OpeningCeremony

After removing the results from legitimate providers like NBCUniversal, the team identified 245 questionable tweets, 23 base accounts promoting free streaming services, and 85 amplifier accounts retweeting free streaming with no apparent relationship to a known legitimate provider.[19] After the Beijing Olympics, the team observed the same Twitter accounts promoting free streaming offers for other sporting events.

18. Ouriel Daskal, "How to solve the problem of piracy in sports broadcasts?," *CTech*, February 18, 2021. (https://www.calcalistech.com/ctech/articles/0,7340,L-3894473,00.html); Henry Bushnell, "Inside the complex world of illegal sports streaming," *Yahoo Sports*, March 26, 2019. (https://www.yahoo.com/now/inside-the-complex-world-of-illegal-sports-streaming-040816430.html)

19. These amplifier accounts may have been a mix of bots, compromised accounts, and "ignorant agents," that is, individuals who retweet information without verifying its authenticity.

How A Digital Footprint Provides A Criminal Foothold

During the Olympics, the tweets directed viewers to intermediate websites offering two options: watch live or register, as seen in Figure 5. Fans who clicked "free register" were directed to another website – landing page – to register and pay a $1 credit card fee for unlimited access, as seen in Figure 6.

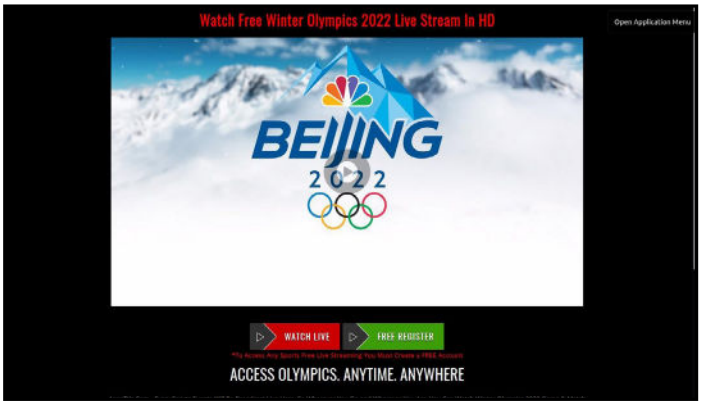


Figure 5: Fraudulent website offering free streaming

Figure 6: Fraudulent website's payment requirement

Security scans of the intermediate website determined it to be malicious, and scans of the landing page assessed that fans would fall victim to a "drive-by compromise" in which malicious software downloads and installs without user permission.[20] Compared to earlier campaigns, criminal actors appear to have refined this fraudulent network, using a single intermediate site and landing page.

A Cypriot company was the registrant for the landing page, which was part of a more extensive network used to spread ransomware and adware, generating millions or even tens of millions of dollars per year. Using DNS and certificate abuse, the operators of the malicious network regularly changed domain names to avoid detection from ad blockers and antivirus software.[21]

The cyber hunt team also discovered the use of plain text code with a newly registered certificate. Analysis of the URL indicated that malware was bundled with the video streams. The malware strands discovered include those associated with the theft of banking information and other data using backdoors and spyware.

Searches for similar domains revealed another website boasting that it ignored the Digital Millennium Copyright Act (DMCA). Clones of this website cluster used domain generation algorithms to rotate domain names to thwart blacklists aimed at protecting users. While illegal video streamers and other malicious actors prefer the .com top-level domain because browsers are less likely to block it, they often create clones using other top-level domains, including .net, .tv, .me, and others.

The site has received hundreds of DMCA violation notices from sports leagues and media companies. The team assessed this likely to be a large, well-funded operation with a significant impact on the sports broadcasting community.

Recommendations

Sports-ISAO provides recommendations to sports leagues, broadcasters, and other global sporting event stakeholders about security and legal remedies to protect the industry. TCIL's recommendations below focus on how to counter malicious actors exploiting operational infrastructure.

20. "Drive-by Compromise," *MITRE ATT&CK*, accessed January 4, 2023. (https://attack.mitre.org/techniques/T1189/)

21. Sports-ISAO Tokyo Olympics Threat Brief # 02A: Video Streaming. Available upon request.

How A Digital Footprint Provides A Criminal Foothold

Expand the Development and Deployment of the DISARM Framework

Understanding how adversaries conduct influence campaigns is critical to countering malicious campaigns. The MITRE Corporation created the ATT&CK standard (Adversary Tactics and Techniques and the Common Knowledge standard, pronounced as "attack") to identify the technical steps adversaries take in each phase of a cyberattack.[22] (See Appendix A.) ATT&CK has become a globally recognized reference for cyberattack techniques to assess how attacks occur and to determine what safeguards protect against the various methods.

While many of the TTPs used in cyberattacks and influence operations overlap — particularly the building of operational infrastructure and other early phases of the campaigns — the ATT&CK framework is not well-suited to other parts of disinformation campaigns.

A working group of the Credibility Coalition developed a counter-disinformation framework to capture the tactics and techniques used to propagate disinformation. The Credibility Coalition is a community of researchers that assesses online information credibility.[23] First published in 2021 as the AMITT (adversarial misinformation and influence tactics and techniques) framework and later renamed DISARM (disinformation analysis and risk management),[24] the framework follows the ATT&CK format by listing an operational sequence of tactics and then listing observed techniques for each tactic. (See Appendix B for the DISARM Framework. DISARM Red identifies adversarial tactics and techniques, while DISARM Blue identifies countermeasures to thwart the adversary's activities.)

The DISARM Framework is on its way to becoming the standard for describing, identifying, disrupting, and countering techniques of influence campaigns. Various agencies worldwide have adopted the framework, including cyber threat intelligence analysts in Taiwan (to analyze Chinese influence operation campaigns),[25] the European External Action Service (to monitor disinformation in Europe),[26] the European Centre of Excellence for Countering Hybrid Threats, and the North Atlantic Treaty Organization's Strategic Communications Centre of Excellence.[27]

Organizations like the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency, the State Department's Global Engagement Center and Technology Engagement Team, the Department of Defense, and U.S. intelligence agencies should adopt and help to further develop the framework. In partnership with researchers, the academic community, and the private sector, the U.S. government should map its identification and countering disinformation operations to a uniform standard.

22. "ATT&CK," *MITRE ATT&CK*, accessed January 4, 2023. (https://attack.mitre.org/)

23. "Credibility Coalition," *Credibility Coalition*, accessed January 4, 2023. (https://credibilitycoalition.org/)

24. "A brief history of DISARM," *DISARM Foundation*, accessed January 4, 2023. (https://www.disarm.foundation/brief-history-of-disarm)

25. SANS Digital Forensics and Incident Response, "Clip Addiction: A Threat Intelligence Approach to Video-Based Chinese InfoOps," *YouTube*, March 25, 2022. (https://www.youtube.com/watch?v=I2gMDEYo2Bo)

26. Interview with Sara-Jayne Terp, May 11, 2022.

27. Hadley Newman, "Foreign information manipulation and interference defence standards: Test for rapid adoption of the common language and framework 'DISARM'," *The European Centre of Excellence for Countering Hybrid Threats* and *NATO Strategic Communications Centre of Excellence*, 2022. (https://stratcomcoe.org/publications/foreign-information-manipulation-and-interference-defence-standards-test-for-rapid-adoption-of-the-common-language-and-framework-disarm-prepared-in-cooperation-with-hybrid-coe/253)

How A Digital Footprint Provides A Criminal Foothold

Throttle Abuse of the Domain Name System (DNS) by Requiring Reseller Certification

The Internet Corporation for Assigned Names and Numbers (ICANN), a nonprofit with multiple stakeholders operating on behalf of the global multistakeholder community,[28] sets global standards for internet protocols. In addition, ICANN maintains the domain name registration process. There are four key players in this process:

1. Registry Operators: ICANN-approved organizations that maintain the master database for a generic top-level domain (gTLD), like .com, .org, or .net
2. Registrars: entities accredited by ICANN to process domain name registrations
3. Resellers: entities contracted to registrars to sell domain names on their behalf
4. Registrants: entities (persons or organizations) looking to procure domain names

Despite maintaining the registration process, ICANN has failed to address how threat actors use certain top-level domains to build malicious infrastructure.

According to ICANN, a new gTLD costs a registrar $185,000 plus $6,250 per quarter.[29] As of 2017, customers could create gTLDs for any reason (for example, for a trademark). This has driven the expansion of registrars and registry operators who allow questionable resellers to provide domain names to various threat actors, including influence operators and cyber criminals. In some cases, these registrars and resellers can be the same entity. Numerous resellers allow the purchase and registration of domains linked to illegal streaming content or malware. If resellers only sold to verifiable entities, threat actors would be less able to exploit DNS for their malicious aims. ICANN should require that all resellers be ICANN certified. To receive and maintain this certification, resellers would need to:

1. Obtain proof of identification before completing a sale (and not use automated registration systems), and
2. Monitor, deny, and report on registration attempts that demonstrate the high levels of activity seen with domain generation algorithms and similar patterns.

Establish International Standards for Vetting Companies Seeking to Become Certificate Authorities

Website certificates digitally link websites with the individuals or organizations that own them. They are necessary to enable secure, encrypted traffic (HTTPS connections). Obtaining certificates used to cost several thousand dollars. Today, it is possible to obtain a certificate for free. This has opened new possibilities for small internet businesses and helped drive encrypted traffic to nearly 90 percent.[30]

The proliferation of certificate authorities (CAs) — and registration authorities (RAs) that purportedly verify the user's identity before authorizing the CA to issue the certificate — has resulted in CAs and RAs that do not conduct the necessary due diligence and verifications. Threat actors can obtain certificates. Most users do not know how to verify certificates manually, leading some to erroneously assume that a website with a lock symbol is safe.

During the Winter Olympics, the team observed a certificate-issuing company and other providers vouching for both legitimate and illicit content. Similar to controls for domain registrations, the certificate issuing process should:

1. Require certificate authorities and registration authorities to obtain registrant proof of identification before completing the certificate issue;

---

28. "Domain Name Registration Process," *ICANN*, accessed January 4, 2023. (https://whois.icann.org/en/domain-name-registration-process)

29. ICANN, *gTLD Applicant Guidebook*, Version 2012-06-04. (https://newgtlds.icann.org/en/applicants/agb/guidebook-full-04jun12-en.pdf)

30. "SSL Inspection (SSLi) Bundles for Scalable Inspection of SSL/TLS Encrypted Traffic," *CISCO Secure*, March 2022. (https://www.cisco.com/c/en/us/products/collateral/security/ssli-bundles-wp.html)

2. Require certificate authorities and registration authorities to monitor, deny, and report entities that abuse certificates; and
3. Establish independent monitoring of Certificate authorities and registration authorities that regularly enable illicit activity and include those sites on public blacklists.[31]

Require Infrastructure-as-a-Service (IaaS) and other Service Providers to "Know Your Customer" and Establish Law Enforcement Frameworks to Prosecute Violators

The pilot and public reporting revealed malicious actors leveraging hosting and security services to shield their activity from blacklists and investigations. Legitimate and illegitimate actors alike utilize off-site servers, cloud storage, and virtual machines that may shield their activity from blacklists and investigations by concealing or limiting access to activity details.

The U.S. government should require service providers to be aware of their clients' identities and cease providing services to customers known to conduct cyberattacks, fraud, or disinformation campaigns. Executive Order 13984 directs the secretary of commerce to issue regulations requiring IaaS providers to conduct due diligence on their customers.[32] Similar measures should be required of hosting and other service providers.

Moreover, Executive Order 13694 authorizes the U.S. Treasury Department to impose financial sanctions on entities found responsible, directly or indirectly, for cyber activities that pose a significant threat to the nation.[33] Treasury has used this authority to sanction cryptocurrency exchanges that knowingly facilitate money laundering and other illicit activity.[34] Treasury should issue guidance clarifying that organizations that run gray infrastructure can be targeted under this executive order.

At the same time, the FBI, U.S. Secret Service, and their international partners, including INTERPOL, should increase investigations and prosecutions of networks that enable a range of illegal activity in cyberspace. This should include identifying known websites conducting malign activity.

Conclusion

Offensive cyber operations and influence operations are not distinct problems requiring different solutions. The pilot demonstrated that influence and cyber operations use similar techniques to build operational infrastructure. Alone, this paper's recommendations will not stop offensive cyber and influence operations. They can, however, provide a blueprint for trusted source validation on the internet. This would allow users to choose more discriminately what sites they visit, who they follow on social media, and what they choose to share online.

31. "Blacklist," *SSL blacklist by ABUSE*, accessed January 4, 2023. (https://sslbl.abuse.ch/blacklist/)

32. U.S. Department of Commerce, Press Release, "Commerce Department Seeks Input in Development of Cyber Rules to Deter Malicious Use of Cloud Services," September 24, 2021. (https://www.commerce.gov/news/press-releases/2021/09/commerce-department-seeks-input-development-cyber-rules-deter-malicious)

33. U.S. Executive Order 13694, "Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities," April 1, 2015. (https://www.federalregister.gov/documents/2015/04/02/2015-07788/blocking-the-property-of-certain-persons-engaging-in-significant-malicious-cyber-enabled-activities)

34. U.S. Department of the Treasury, Press Release, "U.S. Treasury Issues First-Ever Sanctions on a Virtual Currency Mixer, Targets DPRK Cyber Threats," May 6, 2022. (https://home.treasury.gov/news/press-releases/jy0768); U.S. Department of the Treasury, Press Release, "Treasury Takes Robust Actions to Counter Ransomware," September 21, 2021. (https://home.treasury.gov/news/press-releases/jy0364)

How A Digital Footprint Provides A Criminal Foothold

Appendix A: ATT&CK Matrix

Each grouping below represents a tactical goal of the adversary. They can also be linked to the steps of the cyber kill chain. Under each tactic within the tables are the varied techniques observed to achieve the tactical goals.

Source: https://attack.mitre.org/

Reconnaissance

Active Scanning	Gather Victim Host Information	Gather Victim Identity Information	Gather Victim Network Information	Gather Victim Org Information
Phishing for Information	Search Closed Sources	Search Open Technical Databases	Search Open Websites/Domains	Search Open Websites/Domains

Resource Development

Acquire Infrastructure	Compromise Accounts	Compromise Infrastructure	Develop Capabilities	Establish Accounts
Obtain Capabilities	Stage Capabilities			

Initial Access

Drive-by Compromise	Exploit Public-Facing Application	External Remote Services	Hardware Additions	Phishing
Replication Through Removable Media	Supply Chain Compromise	Trusted Relationship	Valid Accounts	

Initial Access

Drive-by Compromise	Exploit Public-Facing Application	External Remote Services	Hardware Additions	Phishing
Replication Through Removable Media	Supply Chain Compromise	Trusted Relationship	Valid Accounts	

Execution

Command and Scripting Interpreter	Container Administration Command	Deploy Container	Exploitation for Client Execution	Inter-Process Communication
Native API	Scheduled Task/Job	Serverless Execution	Shared Modules	Software Deployment Tools
System Services	User Execution	Windows Management Instrumentation		

How A Digital Footprint Provides A Criminal Foothold

Persistence

Account Manipulation	BITS Jobs	Boot or Logon Autostart Execution	Boot or Logon Initialization Scripts	Browser Extensions
Compromise Client Software Binary	Create Account	Create or Modify System Process	Event Triggered Execution	External Remote Services
Hijack Execution Flow	Implant Internal Image	Modify Authentication Process	Office Application Startup	Pre-OS Boot
Scheduled Task/Job	Server Software Component	Traffic Signaling	Valid Accounts	

Defense Evasion

Abuse Elevation Control Mechanism	Access Token Manipulation	BITS Jobs	Build Image on Host	Debugger Evasion
Deobfuscate/Decode Files or Information	Deploy Container	Direct Volume Access	Domain Policy Modification	Execution Guardrails
Exploitation for Defense Evasion	File and Directory Permissions Modification	Hide Artifacts	Hijack Execution Flow	Impair Defenses
Indicator Removal	Indirect Command Execution	Masquerading	Modify Authentication Process	Modify Cloud Compute Infrastructure
Modify Registry	Modify System Image	Network Boundary Bridging	Obfuscated Files or Information	Plist File Modification
Pre-OS Boot	Process Injection	Reflective Code Loading	Rogue Domain Controller	Rootkit
Subvert Trust Controls	System Binary Proxy Execution	System Script Proxy Execution	Template Injection	Traffic Signaling
Trusted Developer Utilities Proxy Execution	Unused/Unsupported Cloud Regions	Use Alternate Authentication Material	Valid Accounts	Virtualization/ Sandbox Evasion
Weaken Encryption	XSL Script Processing			

Credential Access

Adversary-in-the-Middle	Brute Force	Credentials from Password Stores	Exploitation for Credential Access	Forced Authentication
Forge Web Credentials	Input Capture	Modify Authentication Process	Multi-Factor Authentication Interception	Multi-Factor Authentication Request Generation
Network Sniffing	OS Credential Dumping	Steal Application Access Token	Steal or Forge Authentication Certificates	Steal or Forge Kerberos Tickets
Steal Web Session Cookie	Unsecured Credentials			

How A Digital Footprint Provides A Criminal Foothold

Discovery

Account Discovery	Application Window Discovery	Browser Bookmark Discovery	Cloud Infrastructure Discovery	Cloud Service Dashboard
Cloud Service Discovery	Cloud Storage Object Discovery	Container and Resource Discovery	Debugger Evasion	Domain Trust Discovery
File and Directory Discovery	Group Policy Discovery	Network Service Discovery	Network Share Discovery	Network Sniffing
Password Policy Discovery	Peripheral Device Discovery	Permission Groups Discovery	Process Discovery	Query Registry
Remote System Discovery	Software Discovery	System Information Discovery	System Location Discovery	System Network Configuration Discovery
System Network Connections Discovery	System Owner/ User Discovery	System Service Discovery	System Time Discovery	Virtualization/ Sandbox Evasion

Lateral Movement

Exploitation of Remote Services	Internal Spearphishing	Lateral Tool Transfer	Remote Service Session Hijacking	Remote Services
Replication Through Removable Media	Software Deployment Tools	Taint Shared Content	Use Alternate Authentication Material	

Collection

Adversary-in-the-Middle	Archive Collected Data	Audio Capture	Automated Collection	Browser Session Hijacking
Clipboard Data	Data from Cloud Storage	Data from Configuration Repository	Data from Information Repositories	Data from Local System
Data from Network Shared Drive	Data from Removable Media	Data Staged	Email Collection	Input Capture
Screen Capture	Video Capture			

Command and Control

Application Layer Protocol	Communication Through Removable Media	Data Encoding	Data Obfuscation	Dynamic Resolution
Encrypted Channel	Fallback Channels	Ingress Tool Transfer	Multi-Stage Channels	Non-Application Layer Protocol
Non-Standard Port	Protocol Tunneling	Proxy	Remote Access Software	Traffic Signaling
Web Service				

Exfiltration

Automated Exfiltration	Data Transfer Size Limits	Exfiltration Over Alternative Protocol	Exfiltration Over C2 Channel	Exfiltration Over Other Network Medium
Exfiltration Over Physical Medium	Exfiltration Over Web Service	Scheduled Transfer	Transfer Data to Cloud Account	

Impact

Account Access Removal	Data Destruction	Data Encrypted for Impact	Data Manipulation	Defacement
Disk Wipe	Endpoint Denial of Service	Firmware Corruption	Inhibit System Recovery	Network Denial of Service
Resource Hijacking	Service Stop	System Shutdown/Reboot		

Appendix B: DISARM Framework

The DISARM Framework consists of the DISARM Red Framework and the DISARM Blue Framework — both represented below. The Red Framework represents the phases of an influence campaign, with the tactics highlighted in red and the enabling techniques listed below the tactics. The Blue Framework identifies the techniques in each table used to counter the Red Framework tactics shown in blue.

Source: https://disarmframework.herokuapp.com

DISARM Red Framework - incident creator TTPs

PLAN

TA01: Plan Strategy				
T0073: Determine Target Audiences	T0074: Determine Strategic Ends			
TA02: Plan Objectives				
T0002: Facilitate State Propaganda	T0066: Degrade Adversary	T0075: Dismiss	T0075.001: Discredit Credible Sources	T0076: Distort
T0077: Distracta	T0078: Dismay	T0079: Divide		
TA13: Target Audience Analysis				
T0072: Segment Audiences	T0072.001: Geographic Segmentation	T0072.002: Demographic Segmentation	T0072.003: Economic Segmentation	T0072.004: Psychographic Segmentation
T0072.005: Political Segmentation	T0080: Map Target Audience Information Environment	T0080.001: Monitor Social Media Analytics	T0080.002: Evaluate Media Surveys	T0080.003: Identify Trending Topics/Hashtags

How A Digital Footprint Provides A Criminal Foothold

T0080.004: Conduct Web Traffic Analysis	T0080.005: Assess Degree/ Type of Media Access	T0081: Identify Social and Technical Vulnerabilities	T0081.001: Find Echo Chambers	T0081.002: Identify Data Voids
T0081.003: Identify Existing Prejudices	T0081.004: Identify Existing Fissures	T0081.005: Identify Existing Conspiracy Narratives/ Suspicions	T0081.006: Identify Wedge Issues	T0081.007: Identify Target Audience Adversaries
T0081.008: Identify Media System Vulnerabilities				

PREPARE

TA14: Develop Narratives				
T0003: Leverage Existing Narratives	T0004: Develop Competing Narratives	T0022: Leverage Conspiracy Theory Narratives	T0022.001: Amplify Existing Conspiracy Theory Narratives	T0022.002: Develop Original Conspiracy Theory Narratives
T0040: Demand insurmountable proof	T0068: Respond to Breaking News Event or Active Crisis	T0082: Develop New Narratives	T0083: Integrate Target Audience Vulnerabilities into Narrative	

TA06: Develop Content				
T0015: Create hashtags and search artifacts	T0019: Generate information pollution	T0019.001: Create fake research	T0019.002: Hijack Hashtags	T0023: Distort facts
T0023.001: Reframe Context	T0023.002: Edit Open-Source Content	T0084: Reuse Existing Content	T0084.001: Use Copypasta	T0084.002: Plagiarize Content
T0084.003: Deceptively Labeled or Translated	T0084.004: Appropriate Content	T0085: Develop Text-based Content	T0085.001: Develop AI-Generated Text	T0085.002: Develop False or Altered Documents
T0085.003: Develop Inauthentic News Articles	T0086: Develop Image-based Content	T0086.001: Develop Memes	T0086.002: Develop AI-Generated Images (Deepfakes)	T0086.003: Deceptively Edit Images (Cheap fakes)
T0086.004: Aggregate Information into Evidence Collages	T0087: Develop Video-based Content	T0087.001: Develop AI-Generated Videos (Deepfakes)	T0087.002: Deceptively Edit Video (Cheap fakes)	T0088: Develop Audio-based Content
T0088.001: Develop AI-Generated Audio (Deepfakes)	T0088.002: Deceptively Edit Audio (Cheap fakes)	T0089: Obtain Private Documents	T0089.001: Obtain Authentic Documents	T0089.002: Create Inauthentic Documents
T0089.003: Alter Authentic Documents				

TA15: Establish Social Assets				
T0007: Create Inauthentic Social Media Pages and Groups	T0010: Cultivate ignorant agents	T0013: Create inauthentic websites	T0014: Prepare fundraising campaigns	T0014.001: Raise funds from malign actors
T0014.002: Raise funds from ignorant agents	T0065: Prepare Physical Broadcast Capabilities	T0090: Create Inauthentic Accounts	T0090.001: Create Anonymous Accounts	T0090.002: Create Cyborg Accounts
T0090.003: Create Bot Accounts	T0090.004: Create Sockpuppet Accounts	T0091: Recruit malign actors	T0091.001: Recruit Contractors	T0091.002: Recruit Partisans
T0091.003: Enlist Troll Accounts	T0092: Build Network	T0092.001: Create Organizations	T0092.002: Use Follow Trains	T0092.003: Create Community or Sub-group

How A Digital Footprint Provides A Criminal Foothold

T0093: Acquire/ Recruit Network	T0093.001: Fund Proxies	T0093.002: Acquire Botnets	T0094: Infiltrate Existing Networks	T0094.001: Identify susceptible targets in networks
T0094.002: Utilize Butterfly Attacks	T0095: Develop Owned Media Assets	T0096: Leverage Content Farms	T0096.001: Create Content Farms	T0096.002: Outsource Content Creation to External Organizations
TA16: Establish Legitimacy				
T0009: Create fake experts	T0009.001: Utilize Academic/Pseudoscientific Justifications	T0011: Compromise legitimate accounts	T0097: Create personas	T0097.001: Backstop personas
T0098: Establish Inauthentic News Sites	T0098.001: Create Inauthentic News Sites	T0098.002: Leverage Existing Inauthentic News Sites	T0099: Prepare Assets Impersonating Legitimate Entities	T0099.001: Astroturfing
T0099.002: Spoof/parody account/site	T0100: Co-opt Trusted Sources	T0100.001: Co-Opt Trusted Individuals	T0100.002: Co-Opt Grassroots Groups	T0100.003: Co-opt Influencers
TA05: Microtarget				
T0016: Create Clickbait	T0018: Purchase Targeted Advertisements	T0101: Create Localized Content	T0102: Leverage Echo Chambers/Filter Bubbles	T0102.001: Use existing Echo Chambers/ Filter Bubbles
T0102.002: Create Echo Chambers/Filter Bubbles	T0102.003: Exploit Data Voids			
TA07: Select Channels and Affordances				
T0029: Online polls	T0043: Chat apps	T0043.001: Use Encrypted Chat Apps	T0043.002: Use Unencrypted Chats Apps	T0103: Livestream
T0103.001: Video Livestream	T0103.002: Audio Livestream	T0104: Social Networks	T0104.001: Mainstream Social Networks	T0104.002: Dating Apps
T0104.003: Private/Closed Social Networks	T0104.004: Interest-Based Networks	T0104.005: Use hashtags	T0104.006: Create dedicated hashtag	T0105: Media Sharing Networks
T0105.001: Photo Sharing	T0105.002: Video Sharing	T0105.003: Audio sharing	T0106: Discussion Forums	T0106.001: Anonymous Message Boards
T0107: Bookmarking and Content Curation	T0108: Blogging and Publishing Networks	T0109: Consumer Review Networks	T0110: Formal Diplomatic Channels	T0111: Traditional Media
T0111.001: TV	T0111.002: Newspaper	T0111.003: Radio	T0112: Email	

How A Digital Footprint Provides A Criminal Foothold

EXECUTE

TA08: Conduct Pump Priming				
T0020: Trial content	T0039 : Bait legitimate influencers	T0042: Seed Kernel of truth	T0044: Seed distortions	T0045: Use fake experts
T0046: Use Search Engine Optimization	T0113: Employ Commercial Analytic Firms			
TA09: Deliver Content				
T0114: Deliver Ads	T0114.001: Social media	T0114.002: Traditional Media	T0115: Post Content	T0115.001: Share Memes
T0115.003: One-Way Direct Posting	T0116: Comment or Reply on Content	T0116.001: Post inauthentic social media comment	T0117: Attract Traditional Media	
TA17: Maximize Exposure				
T0049: Flooding the Information Space	T0049.001: Trolls amplify and manipulate	T0049.002: Hijack existing hashtag	T0049.003: Bots Amplify via Automated Forwarding and Reposting	T0049.004: Utilize Spamoflauge
T0049.005: Conduct Swarming	T0049.006: Conduct Keyword Squatting	T0049.007: Inauthentic Sites Amplify News and Narratives	T0118: Amplify Existing Narrative	T0119: Cross-Posting
T0119.001: Post Across Groups	T0119.002: Post Across Platform	T0119.003: Post Across Disciplines	T0120: Incentivize Sharing	T0120.001: Use Affiliate Marketing Programs
T0120.002: Use Contests and Prizes	T0121: Manipulate Platform Algorithm	T0121.001: Bypass Content Blocking	T0122: Direct Users to Alternative Platforms	
TA18: Drive Online Harms				
T0047: Censor social media as a political force	T0048: Harass	T0048.001: Boycott/" Cancel" Opponents	T0048.002: Harass People bBased on Identities	T0048.002: Harass People bBased on Identities
T0048.004: Dox	T0123: Control Information Environment through Offensive Cyberspace Operations	T0123.001: Delete Opposing Content	T0123.002: Block Content	T0123.003: Destroy Information Generation Capabilities
T0123.004: Conduct Server Redirect	T0124: Suppress Opposition	T0124.001: Report Non-Violative Opposing Content	T0124.002: Goad People into Harmful Action (Stop Hitting Yourself)	T0124.003: Exploit Platform TOS/Content Moderation
T0125: Platform Filtering				
TA10: Drive Offline Activity				
T0017: Conduct fundraising	T0017.001: Conduct Crowdfunding Campaigns	T0057: Organize Events	T0057.001: Pay for Physical Action	T0057.002: Conduct Symbolic Action
T0061: Sell Merchandise	T0126: Encourage Attendance at Events	T0126.001: Call to action to attend	T0126.002: Facilitate logistics or support for attendance	T0127: Physical Violence
T0127.001: Conduct Physical Violence	T0127.002: Encourage Physical Violence			

How A Digital Footprint Provides A Criminal Foothold

TA11: Persist in the Information Environment				
T0059: Play the long game	T0060: Continue to Amplify	T0128: Conceal People	T0128.001: Use Pseudonyms	T0128.002: Conceal Network Identity
T0128.003: Distance Reputable Individuals from Operation	T0128.004: Launder Accounts	T0128.005: Change Names of Accounts	T0129: Conceal Operational Activity	T0129.001: Conceal Network Identity
T0129.002: Generate Content Unrelated to Narrative	T0129.003: Break Association with Content	T0129.004: Delete URLs	T0129.005: Coordinate on encrypted/closed networks	T0129.006: Deny involvement
T0129.007: Delete Accounts/Account Activity	T0129.008: Redirect URLs	T0129.009: Remove Post Origins	T0129.010: Misattribute Activity	T0130: Conceal Infrastructure
T0130.001: Conceal Sponsorship	T0130.002: Utilize Bulletproof Hosting	T0130.003: Use Shell Organizations	T0130.004: Use Cryptocurrency	T0130.005: Obfuscate Payment
T0131: Exploit TOS/Content Moderation	T0131.001: Legacy web content	T0131.002: Post Borderline Content		

ASSESS

TA12: Assess Effectiveness				
T0132: Measure Performance	T0132.001: People Focused	T0132.002: Content Focused	T0132.003: View Focused	T0133: Measure Effectiveness
T0133.001: Behavior changes	T0133.002: Content	T0133.003: Awareness	T0133.004: Knowledge	T0133.005: Action/attitude
T0134: Measure Effectiveness Indicators (or KPIs)	T0134.001: Message reach	T0134.002: Social media engagement		

DISARM Blue Framework - responder TTPs

TA01: Plan Strategy

C00016: Censorship	C00017: Repair broken social connections	C00019: Reduce effect of division-enablers	C00021: Encourage in-person communication	C00022: Innoculate. Positive campaign to promote feeling of safety
C00006: Charge for social media	C00024: Promote healthy narratives	C00026: Shore up democracy based messages	C00027: Create culture of civility	C00153: Take pre-emptive action against actors' infrastructure
C00096: Strengthen institutions that are always truth tellers	C00111: Reduce polarisation by connecting and presenting sympathetic renditions of opposite views	C00223: Strengthen Trust in social media platforms	C00221: Run a disinformation red team, and design mitigation factors	C00220: Develop a monitoring and intelligence plan
C00212: build public resilience by making civil society more vibrant	C00205: strong dialogue between the federal government and private sector to encourage better reporting	C00190: open engagement with civil society	C00176: Improve Coordination amongst stakeholders: public and private	C00174: Create a healthier news environment
C00170: elevate information as a critical domain of statecraft	C00161: Coalition Building with stakeholders and Third-Party Inducements	C00010: Enhanced privacy regulation for social media	C00073: Inoculate populations through media literacy training	C00012: Platform regulation
C00013: Rating framework for news	C00008: Create shared fact-checking database	C00159: Have a disinformation response plan		

How A Digital Footprint Provides A Criminal Foothold

TA02: Plan Objectives

C00207: Run a competing disinformation campaign - not recommended	C00164: compatriot policy	C00092: Establish a truth teller reputation score for influencers	C00222: Tabletop simulations	C00070: Block access to disinformation resources
C00169: develop a creative content hub	C00060: Legal action against for-profit engagement factories	C00156: Better tell your country or organization story	C00028: Make information provenance available	C00144: Buy out troll farm employees / offer them jobs
C00029: Create fake website to issue counter narrative and counter narrative through physical merchandise	C00030: Develop a compelling counter narrative (truth based)	C00031: Dilute the core narrative - create multiple permutations, target / amplify	C00009: Educate high profile influencers on best practices	C00011: Media literacy. Games to identify fake news

TA05: Microtarget

C00065: Reduce political targeting	C00066: Co-opt a hashtag and drown it out (hijack it back)	C00178: Fill information voids with non-disinformation content	C00216: Use advertiser controls to stem flow of funds to bad actors	C00130: Mentorship: elders, youth, credit. Learn vicariously.

TA06: Develop Content

C00085: Mute content	C00014: Real-time updates to fact-checking database	C00032: Hijack content and link to truth- based info	C00071: Block source of pollution	C00072: Remove non-relevant content from special interest groups - not recommended
C00074: Identify and delete or rate limit identical content	C00075: normalise language	C00076: Prohibit images in political discourse channels	C00078: Change Search Algorithms for Disinformation Content	C00080: Create competing narrative
C00081: Highlight flooding and noise, and explain motivations	C00082: Ground truthing as automated response to pollution	C00084: Modify disinformation narratives, and rebroadcast them	C00086: Distract from noise with addictive content	C00087: Make more noise than the disinformation
C00091: Honeypot social community	C00094: Force full disclosure on corporate sponsor of research	C00106: Click-bait centrist content	C00107: Content moderation	C00142: Platform adds warning label and decision point when sharing content
C00165: Ensure integrity of official documents	C00202: Set data 'honeytraps'	C00219: Add metadata to content that's out of the control of disinformation creators		

TA07: Select Channels and Affordances

C00195: Redirect searches away from DISdisinformation or extremist content	C00098: Revocation of allowlisted or "verified" status	C00105: Buy more advertising than misinformation creators	C00103: Create a bot that engages / distract trolls	C00101: Create friction by rate-limiting engagement
C00097: Require use of verified identities to contribute to poll or comment	C00099: Strengthen verification methods	C00090: Fake engagement system		

How A Digital Footprint Provides A Criminal Foothold

TA08: Conduct Pump Priming

C00117: Downgrade / de-amplify so message is seen by fewer people	C00119: Engage payload and debunk.	C00120: Open dialogue about design of platforms to produce different outcomes	C00121: Tool transparency and literacy for channels people follow.	C00112: "Prove they are not an op!"
C00100: Hashtag jacking	C00154: Ask media not to report false information	C00136: Microtarget most likely targets then send them countermessages	C00188: Newsroom/ Journalist training to counter influence moves	C00184: Media exposure
C00113: Debunk and defuse a fake expert / credentials.	C00114: Don't engage with payloads	C00115: Expose actor and intentions	C00116: Provide proof of involvement	C00118: Repurpose images with new text

TA09: Deliver Content

C00147: Make amplification of social media posts expire (e.g. can't like/ retweet after n days)	C00128: Create friction by marking content with ridicule or other "decelerants"	C00129: Use banking to cut off access	C00182: Redirection / malware detection/ remediation	C00200: Respected figure (influencer) disavows misinfo
C00109: Dampen Emotional Reaction	C00211: Use humorous counter-narratives	C00122: Content moderation	C00123: Remove or rate limit botnets	C00124: Don't feed the trolls
C00125: Prebunking	C00126: Social media amber alert			

TA11: Persist in the Information Environment

C00138: Spam domestic actors with lawsuits	C00139: Weaponise youtube content matrices	C00131: Seize and analyse botnet servers	C00143: (botnet) DMCA takedown requests to waste group time	

TA12: Assess Effectiveness

C00140: "Bomb" link shorteners with lots of calls	C00148: Add random links to network graphs	C00149: Poison the monitoring & evaluation data		

TA15: Establish Social Assets

C00040: third party verification for people	C00059: Verification of project before posting fund requests	C00058: Report crowdfunder as violator	C00172: social media source removal	C00056: Encourage people to leave social media
C00053: Delete old accounts / Remove unused social media accounts	C00052: Infiltrate platforms	C00062: Free open library sources worldwide	C00162: Unravel/target the Potemkin villages	C00067: Denigrate the recipient/ project (of online funding)
C00189: Ensure that platforms are taking down flagged accounts	C00051: Counter social engineering training	C00160: find and train influencers	C00197: remove suspicious accounts	C00077: Active defence: run TA15 "develop people" - not recommended
C00036: Infiltrate the in-group to discredit leaders (divide)	C00203: Stop offering press credentials to propaganda outlets	C00048: Name and Shame Influencers	C00047: Honeypot with coordinated inauthentics	C00155: Ban incident actors from funding sites
C00046: Marginalise and discredit extremist groups	C00093: Influencer code of conduct	C00042: Address truth contained in narratives	C00135: Deplatform message groups and/or message boards	C00133: Deplatform Account*
C00044: Keep people from posting to social media immediately	C00034: Create more friction at account creation			

Acknowledgments

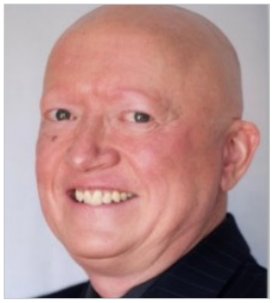
Thank you to the Sports-ISAO team — Doug, Jane, Stephen, Brad, and Christopher — for your contributions and expertise. It was a pleasure working with you and taking advantage of your Winter Olympics mission to demonstrate the similarities of the enabling infrastructure required for influence and cyber operations.

Thank you, Jon Brewer, for reviewing the paper and your work on the DISARM framework. It is a much-needed standard, and I look forward to seeing its progression.

Sports ISAO Team

Doug M. DePeppe, Esq.
Founder of the Cyber Resilience Institute and Co-founder of its Sports-ISAO

R. Jane Ginn
Co-founder of Sports-ISAO



Stephen H. Campbell
Lead Social Media Threat Hunter

Brad E. Rhodes
Lead Cyber Observable Threat Hunter

Christopher Robinson
Cyber Observable Threat Hunter

How A Digital Footprint Provides A Criminal Foothold

About the Author

Dr. Georgianna "George" Shea serves as chief technologist for FDD's Center on Cyber and Technology Innovation and TCIL. In that role, she identifies cyber vulnerabilities in the U.S. government and private sector, devising pilot projects to demonstrate feasible technology and non-tech solutions that, if scaled, could move the needle in defending U.S. prosperity, security, and innovation.

About the Foundation for Defense of Democracies

FDD is a Washington, DC-based, nonpartisan 501(c)(3) research institute focusing on national security and foreign policy.

About FDD's Transformative Cyber Innovation Lab

TCIL finds and nurtures technologically feasible, testable pilot projects which begin to solve some of the hardest cyber problems afflicting the national security industrial base and the United States. TCIL's mission is to help shorten the lag between idea and piloting and between piloting and the adoption of potential solutions to the thorniest of cyber problems. TCIL seeks to drive revolutionary, society-wide improvement in cyber resilience through the innovative synthesis of technology, policy, and governance.

For more information, visit: https://www.fdd.org/projects/transformative-cyber-innovation-lab

About FDD's Barish Center for Media Integrity

FDD's Barish Center for Media Integrity addresses the national security threats posed by misinformation, disinformation campaigns, and influence operations waged by foreign adversaries against the United States and allied democracies.

For more information, visit: https://www.fdd.org/projects/barish-center-for-media-integrity/