2020 12th International Conference on Cyber Conflict
20/20 Vision: The Next Decade
T. Jančárková, L. Lindström,
M. Signoretti, I. Tolga, G. Visky (Eds.)
2020 © NATO CCDCOE Publications, Tallinn

Defenders Disrupting Adversaries: Framework, Dataset, and Case Studies of Disruptive Counter-Cyber Operations

Jason Healey
Senior Research Scholar
School of International and
Public Affairs
Columbia University
New York, NY, United States
jh3639@sipa.columbia.edu

Neil Jenkins
Chief Analytic Officer
Cyber Threat Alliance
Arlington, VA, United States
neiljenkins@cyberthreatalliance.org

JD Work
Bren Chair, Cyber Conflict and Security
US Marine Corps University
Quantico, VA, United States
JW3646@columbia.edu

Abstract: Over the past two decades, there have been numerous defensive operations to disrupt malicious cyber activity by hacktivists, criminals, and nation-state actors. Disruption operations seek to affect the adversary's decision-making processes and impose additional costs. Such operations include a wide range of actions, from releasing indicators of compromise and naming-and-shaming, to botnet and infrastructure takedowns, to indictments and sanctions, and may be conducted outside of the defender's own network with the intent to interrupt adversary cyber offense and espionage. The United States Department of Defense recently released a new strategy that calls for "persistent engagement" with malicious cyber actors, suggesting many more disruption operations to come.

In this paper, we describe a framework for categorizing disruption operations and their effects – along with detailed descriptions for several of these case studies coded to the framework – so that researchers and practitioners can measure their impact using a common terminology. We also provide a unique dataset of over 100 cases of defensive operational disruption over the last 30 years, from 1987 through 2019.

We believe that providing a more complete vocabulary for disruptive operations will give analysts and researchers a better opportunity to compare the different types and effects of various disruption operations. Ideally, this will then provide defenders with the information they need to conduct disruption operations at greatest scale, least cost, and with the lowest chance of escalation.

Keywords: *offensive cyber, counter-cyber, takedown, disruption*

1. INTRODUCTION

The United States military has reoriented its role in order to emphasize a "persistent presence" to "intercept and halt cyber threats" with the hope of countering "malicious cyber activity in day-to-day competition".[1] Through persistent engagement, the DoD will employ defensive cyber operations to disrupt adversaries' operations directly and impose friction so they will be forced to spend more resources on defense, rather than offense.[2]

However, there is no public methodology that can measure the effectiveness of such disruptive operations. Without a measurement methodology, analysts cannot reliably assess the success of this policy or compare the effectiveness of different kinds of disruptive operations. Building upon earlier work by Healey and Jenkins in measuring the effects of persistent engagement, this study builds toward understanding the real-world impacts of such operations.[3] This paper begins by describing an analytical framework for assessing disruption operations, which is followed by an assessment of five cases using the framework, including a unique dataset of 100+ such cases. A concluding section summarizes the insights, future research, and conclusions.

1 Department of Defense. *Cyber Strategy*. 18 September 2018.
2 Jason Healey, "The Implications of Persistent (and Permanent) Engagement in Cyberspace," *Journal of Cybersecurity*. 5, no. 1 (2019).
3 Jason Healey, Neil Jenkins. "Rough-and-Ready: A Policy Framework to Determine if Cyber Deterrence is Working or Failing." *11th International Conference on Cyber Conflict: Silent Battle. Tallinn, Estonia. 28-31 May 2019*.

Though these are still early steps, our goal is to encourage transparency and repeatability to better characterize and understand the scope and range of disruptive counter-cyber operations. We explore the factors that lead to the "most effective" disruption outcomes, although a more complete assessment is out of the scope of this paper. In general, we anticipate that disruptive actions that are more active, more collaborative, more frequent, and more intrusive will have greater impact. But we recognize that mere attrition is not the only measure of effect, as some disruptive actions will likely offer more decisive effect at some substantive threshold, or within particularly operationally relevant timeframes. We anticipate that the elements contributing to successful disruption outcomes will vary across differing situations, and that while a simplified generalization of best choices is not likely possible, there are specific most-effective approaches for a given type of disruptive activity.

2. ANALYTICAL FRAMEWORK

Disruptive counter-cyber operations are positive steps for defeating a specific cyber adversary, usually taken by defenders in response to a specific attack or campaign, and they often directly disrupt an adversary's technology; the main action is typically either outside of the defender's own network or based on specific intelligence about how that adversary operates. This is only a general description, as each element of that description contains important exceptions, so we will examine each part individually:

1. **Positive steps to defeat a *specific* cyber adversary**, usually but not always conducted online. It would not include best-practice defensive measures, such as patching computers, unless specifically intended to defeat a particular adversary that is known or suspected to be targeting that vulnerability. Disruptive operations are generally marked by *active contention* with an adversary.
2. **Usually taken by a defender**, such as a government, cybersecurity, or technology company, or the victim of an attack. There are rare exceptions, such as examples of so-called red-on-red operations where two maliciously motivated actors contest control of infrastructure for their own objectives that remain at odds with the victim's interests.
3. **Taken in response to a specific cyber attack or campaign** to disrupt an adversary's ability to continue ongoing action. This distinguishes it from offensive cyber effects operations (which may come before, during, or after a campaign and serve different purposes), pure retaliation (which is meant to punish for past, not disrupt ongoing, behavior), or deterrence-by-punishment (which is intended primarily to punish an adversary to change their decision calculus). This framework is only, for now, interested in *disrupting* cyber

activities (such as disruptive attacks or intrusions) and not *influence* or *information* operations. We include some actions, such as law-enforcement indictments, in this framework, which may take place well after a campaign. However, these share enough other characteristics with other disruptive operations to be usefully included.

4. Often **directly disrupt an adversary's technology** and typically the **main action is outside of the defender's own network** or **based on specific intelligence** about how the adversary operates. A botnet takedown disrupts technology outside the network of most defenders, while cybersecurity companies and infrastructure sectors share, routinely and at massive scale, their insights of adversary groups to block their efforts on defenders' internal networks.

We evaluate such disruptive operations through a framework of multiple factors related to execution, approach, impact, and adversaries. This framework is neither a formal taxonomy nor has it matured through extended use by analysts; rather it is intended as a first draft of an analytical tool.

A. Dependent Variable: Effect and Duration of Disruption

The effectiveness of disruptive operations is the dependent variable, the thing we want to explain. It can be assessed in at least two ways, a simple description of the impact as well as an estimate of how long it takes the adversary to return to initial operating capability (able to conduct some limited operations) and return to full operating capability (approaching the full range of the adversary's previous activity). These measures of effect and duration overlap; and with use, it may be obvious which of these two is most useful. As that is not yet clear, both are included here.

Effect can be described by a simple three-point scale:

- *Minor*: Slight impact to adversary operations;
- *Significant*: Intermediate impact;
- *Decisive*: Substantive impact.

Duration can be hard to measure, so is simplified to a four-point scale:

- Days to weeks;
- Weeks to months;
- Months to years;
- Never.

A disruption might be so massive that the adversary group disbands. In these cases, the mission, personnel, tools, or infrastructure may be handed off to other groups associated with a particular nation or group, which can confound this assessment.

The other elements of the framework categorize the independent variables, those which will be studied for the impact on the effectiveness of this dependent variable of disruption.

B. Independent Variables

1) Type of Disruption

Technical measures to disrupt adversaries cover a wide spectrum and can usefully be categorized in many ways. For example, disruptive operations can be categorized by the *functional object* at which they are targeted:

- Systems and infrastructure in blue space (that is, owned or operated by the defenders);
- Systems and infrastructure in gray space (owned by neither defenders nor adversary);
- Systems and infrastructure in red space (owned or operated by the adversary);
- Command-and-control (C2) capabilities;
- Adversary personnel;
- Adversary organizations;
- Adversary leadership.

Another categorization is by the *action*, from relatively passive to far more active measures:[4]

- Sinkhole traffic;
- Share threat intelligence with closed trust group (multiple security actors);
- Publicly disclose indicators of compromise;
- Publicly release adversary toolset;
- Publish comprehensive report on malicious cyber activity and mitigations;
- Build protections for security products based on observed indicators of compromise and behaviors (single actor);
- Synchronize the deployment of protections (multiple actors);
- Coordinate vulnerability patching or other protections;
- Disrupt criminal channels for distribution or monetization;
- Force uninstall/deletion/takeover of malware;
- Seize control of adversary C2 nodes or network;

4 The authors have conducted an initial cross-linking of these actions against the Lockheed Martin's Cyber Kill Chain, though it is not included here for brevity. While useful, frameworks like the kill chain have some limitations as they are private-sector focused and lack a feedback loop through which to include the impact of disruptive actions.

- Seize domains used by adversaries;
- Counter-offensive operations to directly target intermediate infrastructure;
- Counter-offensive operations to disrupt attackers' home networks;
- Seizure or kinetic destruction of servers or infrastructure.

Disruptive actions also can be directed not at an adversary's technical infrastructure but their *decision making*:

- Publicly disclose the identities or organizational affiliation of the adversaries;
- Publicly disclose the nation responsible;
- Diplomatic démarche;
- Law-enforcement indictment and prosecution;
- Influence operations against individuals, organizations, or leadership;
- Deception operations;
- Economic sanctions;
- Military options (kinetic or cyber) to coerce adversary to desist.

These actions reflect a range of defensive cyber operations measures, response actions and other counter-cyber operations options, and full offensive employment approaches. These are commonly defined within the US Department of Defense and allied doctrine, which in turn is adopted directly or through influence of common practice by other actors across the environment.[5] The decision to select one set of options versus another is highly case-specific. This decision is influenced by the identity and available authorities of the disrupting actor, available technical capacity and talent, target-specific vulnerabilities and operational security failures, adversary organizational and process considerations that may be variably exploited, as well as temporal considerations.

2) Frequency of Disruptive Activity
Disruptive operations can take place with different frequencies:

- *One-off*: Disruptive activity is only conducted once;
- *Periodic*: Related set of disruptive activities taking place occasionally over time;
- *Sustained*: Related set of disruptive activities taking place frequently and in a coordinated manner.

3) Potential Reasons for Delay in Returning to Operations
Adversaries may not return to full operating capability for reasons only loosely related to the disruptive action. Accordingly, any analytical framework must include some

5 Department of Defense. *Cyberspace Operations*. Joint Publication 3–12. 8 June 2018.

way to include such assessments lest defenders misunderstand the actual impact of their operations. These factors include the following:

- *Technical*, for example from having attack infrastructure burned;
- *Behavioral*, such as if adversaries shift to a different, less fruitful, target set;
- *Bureaucratic*, perhaps from a re-organization once certain adversary teams were publicly called out;
- *Political*, for example if adversary leadership shift operations to favor other domestic interest groups or cut down on operations seemingly out of their control or linked to corruption;
- *Geopolitical*, if an adversary fears backlash for operating against another nation.

4) Geopolitical Context of Disruption
Analysts must also distinguish the geopolitical context of the disruptive operation, which will often have significant explanatory power as other elements:

- *Peace*: Lack of any significant military or diplomatic confrontation;
- *Tension*: Increase of military or diplomatic confrontation but unlikely to escalate into war without significant additional degradation;
- *Crisis*: Significant, acute military or diplomatic confrontation, especially with a chance of war or substantial national interests at stake;
- *War*: Active and routine military operations by the participants.

5) Type of Adversary
Lastly, the framework must distinguish both what kind of organization is conducting the disruption and what kind is being disrupted:

- Disrupt*ed* actor (adversary): state/non-state, criminal or geopolitical aims, relative cyber maturity, relations with other adversary groups, etc.;
- Disrupt*ing* actor: state, major technology company, geopolitical, coalition of states, coalition of technology groups, public–private sector partnership (PPP), etc.

3. CASE STUDIES OF DISRUPTIVE COUNTER-CYBER OPERATIONS

Multiple incidents provide ample fodder for case analysis to use this framework. This section first introduces our dataset (see Table 1 below), consisting of over 100 cases of defensive operational disruption over 30 years, from 1987 through 2019, and then

explores five case studies. These cases were selected based on industry intelligence reporting and information security literature, in which specific actions were noted to have had impact on adversary evolution, changing capabilities and intentions, or future operational planning for later disruption actions. While the influence of these cases can be traced in multiple intelligence and operational contexts, no prior effort to systematically assemble, document, and assess the corpus in total could be identified.

The limitations of space preclude comprehensive examination of each incident. Each case arose within the context of a specific threat exploiting discrete vulnerabilities to deliberate effect, often reported on over months or years in a body of work that alone may fill entire volumes. However, several cases are especially relevant as illustrative examples of the proposed assessment framework.

Eviction of CodeRed Worm: "White worm" inoculated vulnerable systems by unknown and red-on-red actors (rows 4-6 in dataset)

The widespread propagation of the CodeRed worm across Microsoft Internet Information Services (IIS) servers vulnerable to CVE-2001-0500 in July 2001 was a formative event for many cybersecurity professionals, and was among the first incidents in which political motivations were widely considered due to geographic references left in the malware itself. The incident drove substantial efforts toward information sharing, collaborative defense, and crisis management practices that remain fundamental to the industry. However, a perceived lack of effective government response further drove early vigilante efforts to degrade the effectiveness of adversary action, resulting in the release of one of the earliest examples of "white worm" deployment, in which payloads intended to inoculate vulnerable systems were released into the wild by unknown actors – without the consent of system owners. Ultimately, the CodeGreen "vaccination" campaign would itself serve as a model for further adversary abuse where other adversary actors sought to deliver their own wormable payloads exploiting the same vulnerabilities – evicting CodeRed infections but also delivering control of these systems to other operators with hostile intent in one of the earliest documented adversary on adversary (red-on-red) campaigns.[6] The case, despite its age and some complexity across multiple incident phases, remains significant, as both criminal and advanced persistent threat group predation on other vulnerable bad actors continues to surface as an ongoing feature of the contemporary cyber environment.

6 David Moore, Colleen Shannon, and K. Claffy. "Code-Red: A Case Study on the Spread and Victims of an Internet Worm." *Proceedings of the 2nd ACM SIGCOMM Workshop on Internet measurement (IMW). Marseille France. November 2002.*; Nicholas Weaver, Vern Paxson, Stuart Staniford, and Robert Cunningham. "A Taxonomy of Computer Worms," *WORM '03: Proceedings of the 2003 ACM Workshop on Rapid Malcode, Washington, DC, USA, 27 October 2003*, https://doi.org/10.1145/948187.948190.

- Effect and duration of disruption: Minor; while the white worms reduced the pool of some vulnerable systems, the scale of overall vulnerability still resulted in substantial adversary freedom of action;
- Type of disruption: Forced uninstall/deletion/takeover of malware;
- Frequency of disruption: Sustained (for inoculated systems);
- Potential reasons for delay: Technical;
- Geopolitical context: N/A;
- Type of adversaries: Criminal, Unknown and red-on-red.

Conficker Disruption: long-term counter-malware campaign (row 21 in dataset)

The sustained, multi-stakeholder effort required to disrupt widespread infections of the serial version of the Conficker malware family provides an instructive case of effective disruption operations involving large scale, rapidly evolving threats. The years-long efforts of a group of quiet professionals, often working with only limited government support and against a backdrop of serious litigation, policy, and financial risks, is the stuff of legends among the infosec community.[7] They employed counter-measures – especially sink-holing operations – to halt propagation and defeat hostile administration of compromised victims through seizing domain registration, which was complicated by the wide, algorithmically derived namespace used for malware C2. The ultimate resolution of this case is intertwined in subsequent exploitation of common vulnerabilities, to the point that the arrests of several Conficker operators in the Ukraine passed largely unnoticed.[8] The ability of the disruption operators to generate and maintain pressure on the botnet severely limited the adversary's ability to leverage any utility of what was an innovative and even surprising design.[9]

- Effect and duration of disruption: Significant, weeks to months;
- Type of disruption: Botnet takedown with multiple active and passive measures, targeting technical infrastructure and actions in blue, gray, and red space;[10]
- Frequency of disruption: Sustained;
- Potential reasons for delay: Technical;
- Geopolitical context: N/A;
- Type of adversaries: Criminal, PPP.

7 Mark Bowden, *Worm: The First Digital World War* (London: Atlantic Books, 2012).

8 Brian Krebs, "$72M Scareware Ring Used Conficker Worm," *Krebs on Security*, June 2011, https://krebsonsecurity.com/2011/06/72m-scareware-ring-used-conficker-worm/#more-10417.

9 Dave Piscitello, "Conficker Summary and Review," *ICANN*, 7 May 2010, https://www.icann.org/en/system/files/files/conficker-summary-review-07may10-en.pdf.

10 The formulation of blue, gray, and red network space is taken from current USG operational thinking, which makes key distinctions between friendly (blue) and adversary systems and networks (red), as those which are effectively uncontrolled (gray).

GameOverZeus Takedown: heavily coordinated takedown of a botnet by a public–private partnership (row 56 in dataset)

Operation Tovar, the takedown against the GameOverZeus botnet in June 2014, was more technically complex than any preceding it, due to the resilient peer-to-peer C2 architecture, itself evolved under earlier and continuing administrative, technical, and law-enforcement pressures. The botnet was disrupted through cryptanalytic attack under judicial authorities, exploiting weaknesses in C2 protocol to contest adversary control of infected bots through forged commands issued via disruptive nodes introduced into peer-to-peer exchange. As a result of worldwide law-enforcement actions coordinated with technical action, the adversary was unable to resist loss of infrastructure.[11] However, this action may have represented the high water mark for law-enforcement-led, public-private partnerships to counter malicious infrastructure, as it has been suggested that subsequent takedown efforts have been increasingly less effective over time.[12]

- Effect and duration of disruption: Decisive, months to years;
- Type of disruption: Botnet takedown with multiple parallel active measures against technical infrastructure, owned by adversary;
- Frequency of disruption: One-off;
- Potential reasons for delay: Technical;
- Geopolitical context: N/A;
- Type of adversaries: Criminal, PPP.

China-Related Disclosures: public disclosure of cyber espionage (rows 45, 55, 65, 82, and 91 in dataset)

Public attribution linking Chinese operators to ongoing intrusion campaigns remains a vital tool for many states seeking to challenge the undesirable behavior of competitors in the court of public opinion, intended to impose political costs on adversary actors as well as their sponsors and leaders.[13] There is some evidence to suggest that the sequential impact of mere disclosure may be attenuated when hostile services are repeatedly accused – whether through *name and shame* as an influence tactic, or even indictments under judicial process. The initial disclosures linking the APT1 / Comment Crew intrusion set to the operations of a specific People's Liberation Army unit had

11 Europol, "International Action Against 'Gameover Zeus' Botnet And 'Cryptolocker' Ransomware," News release, (2 June 2014).; Symantec, "International Takedown Wounds Gameover Zeus Cybercrime Network," News release, (2 June 2014).; Brian Krebs, "'Operation Tovar' Targets 'Gameover' ZeuS Botnet, CryptoLocker Scourge," *Krebs on Security*, (2 June 2014), https://krebsonsecurity.com/2014/06/operation-tovar-targets-gameover-zeus-botnet-cryptolocker-scourge/.

12 Brandon Levene, "Crimeware in the Modern Era: A Cost We Cannot Ignore," *Chronicle*, 5 September 2019.

13 Florian J. Egloff and Andreas Wenger, "Public Attribution of Cyber Incidents," *Center for Security Studies, ETH Zurich. May 2019*.

substantial diplomatic impact.[14] It is likely that the multi-year reverberations of this action were a contributory factor to the 2015 agreement between Xi and Obama to prohibit further economic espionage, wherein both sides agreed that "neither country's government will conduct or knowingly support cyber-enabled theft of intellectual property, including trade secrets or other confidential business information, with the intent of providing competitive advantages to companies or commercial sectors."[15]

The sequential disclosures of multiple intrusion sets attributed to the Ministry of State Security – including APT3 / GOTHIC PANDA / UPS TEAM, APT10 / STONE PANDA / MenuPass / POTASSIUM, and APT17 / AURORA PANDA / DOGFISH – each challenged the earlier narrative of diplomatic agreement, in which China was seen as a reformed actor, adhering however loosely to the spirit of the negotiation.[16] Industry reporting on these intrusion sets' victims, accesses, and action objectives was matched by an unknown third party disclosure offering substantial attribution detail, followed by Department of Justice indictments.[17] Open questions remain, however, as to whether this strategic impact translates to operational disruption effect.

- Effect and duration of disruption: Unknown;
- Type of disruption: Disclosure;
- Frequency of disruption: Periodic;
- Potential reasons for delay: Bureaucratic (intelligence gain / loss considerations, diplomatic concerns);
- Geopolitical context: Tension (great power competition);
- Type of adversaries: State intelligence, State intelligence / Law Enforcement, unknown actor(s).

Joanap Takedown: government takedown of botnet (row 94 in the dataset)

The Joanap botnet was a component of the infrastructure used by the DPRK-attributed HIDDEN COBRA / LAZARUS intrusion set for reconnaissance, staging, and

14 FireEye, "APT1," 19 February 2013, https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf.

15 White House, "FACT SHEET: President Xi Jinping's State Visit to the United States," 25 September 2015, https://obamawhitehouse.archives.gov/the-press-office/2015/09/25/fact-sheet-president-xi-jinpings-state-visit-united-states.

16 FireEye, "Red Line Drawn: China Recalculates Its Use of Cyber Espionage," 21 June 2016; Robert Farley, "Did the Obama-Xi Cyber Agreement Work?" *The Diplomat*, 11 August 2018.; Herb Lin, "What the National Counterintelligence and Security Center Really Said About Chinese Economic Espionage," *Lawfare*, 31 July 2018.

17 DOJ, "U.S. Charges Three Chinese Hackers Who Work at Internet Security Firm for Hacking Three Corporations for Commercial Advantage," 27 November 2017. https://www.justice.gov/opa/pr/us-charges-three-chinese-hackers-who-work-internet-security-firm-hacking-three-corporations; Cristiana Brafman Kittner and Ben Read. "Red Line Redrawn: China APTs Resurface," *FireEye Cyber Defense Summit. Washington, DC. 1-4 October 2018*.; DOJ, "Two Chinese Hackers Associated with the Ministry of State Security Charged with Global Computer Intrusion Campaigns Targeting Intellectual Property and Confidential Business Information," 20 December 2018. https://www.justice.gov/opa/pr/two-chinese-hackers-associated-ministry-state-security-charged-global-computer-intrusion

distributed denial of attack (DDOS) actions, leveraging previously infected victim systems at scale for multiple global operations since at least 2009.[18] The infrastructure was reportedly quite aged at the time of the January 2019 takedown operation by the Department of Justice and Air Force Office of Special Investigations, and considered "not that interesting" by industry researchers.[19] Still, the takedown action against this legacy infrastructure precluded adversary options to later revive it, especially under the continuing pressure of other ongoing countering options intended to deny and degrade North Korea's cyber operations posture. And even if the adversary had not intended to return this legacy inventory of compromised bots to active use, the takedown effort to disrupt potential hostile use of these bots may be viewed in analogy to removing unexploded ordnance. While removing unexploded ordnance may not be considered the most impactful mechanism in a contest with an adversary offensive program, such actions have undeniable value for the stability of the global cyberspace ecosystem as a whole.

- Effect and duration of disruption: Decisive, months to years;
- Type of disruption: Botnet takedown;
- Frequency of disruption: One-off;
- Potential reasons for delay: Technical and bureaucratic (may not have been worth devoting resources to building an obsolete network);
- Geopolitical context: Tension;
- Type of adversaries: State intelligence, law enforcement.

4. DATASET OF OPERATIONAL DISRUPTION

A full coding of all 100+ cases in this framework is outside the scope of the current paper. Rather we have used a simplified coding, starting with a common name for the operation or disrupted group and the approximate date of the operation. The third column codes the motivation of the disrupted adversary, whether criminal, hacktivist, espionage, or strategic attack. Motivation is coded based on contemporaneous reporting assessment by the security researchers, commercial intelligence firms, or government actors involved in the action. While this potentially omits later understanding of complex motivations developed through deeper historical analysis, it does capture the then-dominant consensus views and therefore the key influences involved in disruption actions at the time when these decisions were taken.

In a few cases, the disruption was not related to targeting an adversary but had another purpose, such as inoculation, essentially intruding into others' vulnerable devices to pre-emptively patch them against the truly malicious. Those cases are coded as

18 DHS CISA, "HIDDEN COBRA – Joanap Backdoor Trojan and Brambul Server Message Block Worm," 29 May 2018, https://www.us-cert.gov/ncas/alerts/TA18-149A.

19 Amit Serper. ""Hmm wait. This is ancient stuff, from like... errr... Almost 7 years ago. OTH, not that interesting?" 4 June 2018, Twitter, https://twitter.com/0xAmit/status/1003742265762811905.

vulnerability reduction.[20] The last column codes the actor conducting the disruption: industry, government, or public-private partnerships. A small number of cases are red-on-red incidents between malicious adversary operators. Those coded as government can be further specified as intelligence, military, law enforcement (LE), or national Computer Emergency Response Teams (CERT).[21] However, to date, we have only documented LE cases. In some LE cases, the originating investigations may have been enabled by unacknowledged industry support, and government intelligence services may play an unacknowledged role in many other cases in ways that have not been publicly documented to date. No unilateral CERT actions have as yet been identified in these cases, likely due to the collaborative nature of these organizations' work processes in coordinating action on private sector networks, inherently involving public-private partnership. Despite this, some unilateral responses may be contemplated and the option to recognize these edge cases is preserved. The dataset deliberately excludes actions to counter hostile influence operations and other coordinated inauthentic activity conducted through cyber platforms, as we are focusing for now on "hard" offensive cyber interactions.

The dataset is skewed toward open-source reporting, as industry and law enforcement often disclose operations for public relations value.[22] Longer-term exploitation of targeted adversary infrastructure through counter-cyber network exploitation (CCNE) operations is likely underrepresented, including in LE cases where employment of active network investigative techniques may have preceded takedown actions.[23] The use of such techniques has been documented in multiple contexts, but, due in no

20 Nicholas Weaver, Vern Paxson, Stuart Staniford, and Robert Cunningham. "Large Scale Malicious Code: A Research Agenda," DARPA, 2003.; Bruce Schneier, "Benevolent Worms," *Crypto-Gram*, 14 September 2003.; Frank Castaneda, Emre Can Sezer and Jun Xu. "WORM vs. WORM: Preliminary Study of an Active Counter-Attack Mechanism," *ACM workshop on Rapid Malcode (WORM), Washington, DC, 29 October 2004*.; Mason J. Molesky and Elizabeth A. Cameron, "Internet of Things: An Analysis and Proposal of White Worm Technology," *IEEE International Conference on Consumer Electronics (ICCE). Las Vegas, NV 11-13 January 2019*.

21 CERT organizations may exist under numerous bureaucratic frameworks that vary by state, and some are even operated by private sector actors. Here, however, we consider the functional role of independent national entities intended to coordinate response to ongoing cyber incidents for enterprise or sector level availability, integrity, and confidentiality objectives vice intended prosecution or intelligence objectives.

22 Clement Guitton, "Criminals and Cyber Attacks: The Missing Link between Attribution and Deterrence," *International Journal of Cyber Criminology* 6, no. 2 (July – December 2012): 1030–43.

23 Brian L. Owsley, "Beware of Government Agents Bearing Trojan Horses," *Akron Law Review* 48, no. 2 (2015).; Jonathan Mayer, "Government Hacking," *Yale Law Journal* 127, no. 3 (2017).; Eduardo R Mendoza. "Network Investigation Techniques: Government Hacking and the Need for Adjustment in the Third-Party Doctrine," *St Mary's Law Journal*, 49 (2017).; Christine W. Chen, "The Graymail Problem Anew in a World Going Dark: Balancing the Interests of the Government and Defendants in Prosecutions Using Network Investigative Techniques," *Columbia Science & Technology Review* XIX (Fall 2017).; Paul Ohm, "The Investigative Dynamics of the Use of Malware by Law Enforcement," *William & Mary Bill of Rights Journal* 26, no. 2 (2017).; Brian L. Owlsey, "Network Investigative Source Code and Due Process," *Digital Evidence and Electronic Signature Law Review* 14 (2017).

small part to continuing legal controversy, these actions are rarely highlighted in post-takedown case summaries.[24]

The dataset also omits routine takedown operations intended to counter ephemeral abuse and simple malicious hosting, as is commonly used in phishing, drive-by malware distribution, secondary payload staging, exfiltration drops, or other tactical functions by actors who anticipate prompt pressure upon use, and therefore are rotated with relatively high frequency. (The dynamics of this tactical level chase are well captured in the "Pyramid of Pain" analytic construct.)[25] Red-on-red cases are also likely underrepresented, due to limited observation and unwillingness of victims to provide any public disclosure.

Disruptive counter-cyber operations can be targeted across malware, command-and-control, and other supporting infrastructure, adversary operator freedom of action, or enabling transactional marketplaces. The differing nature of these defensive objectives plays a role in the effectiveness, or lack thereof, of disruptive counter-cyber disruptions. Simple prediction or even ready explanations of disruptive outcomes are clouded by these differing targeting objectives, sensitivity to initial conditions, and other case-specific factors.

TABLE 1: DATASET OF CYBER DISRUPTION EVENTS

#	Disruptive Event or Campaign	Approximate Date	Motivation of Disrupted Adversary	Disruption Actor
1	Anti-Christma Exec probable campaign[i]	December 1987	Vuln Reduction	Industry
2	Denzuko campaign targeting Brain[ii]	March 1988	Criminal	Red-On-Red
3	Cheese campaign targeting L1on[iii]	May 2001	Vuln Reduction	Unknown
4	CodeGreen campaign targeting CodeRed[iv]	September 2001	Vuln Reduction	Unknown
5	CRClean campaign targeting CodeRed[v]	September 2001	Vuln Reduction	Unknown
6	Klez campaign targeting CodeRed[vi]	October 2001	Criminal	Red-On-Red

24 Brian L. Owsley, "Beware of Government Agents Bearing Trojan Horses," *Akron Law Review* 48, no. 2. (2015).; Jonathan Mayer, "Government Hacking." *Yale Law Journal*, 127, no. 3. 2017.; Eduardo R Mendoza, "Network Investigation Techniques: Government Hacking and the Need for Adjustment in the Third-Party Doctrine," *St Mary's Law Journal*. 49 (2017).; Christine W. Chen, "The Graymail Problem Anew in a World Going Dark: Balancing the Interests of the Government and Defendants in Prosecutions Using Network Investigative Techniques," *Columbia Science & Technology Review* XIX (Fall 2017).; Paul Ohm, "The Investigative Dynamics of the Use of Malware by Law Enforcement," *William & Mary Bill of Rights Journal* 26, no. 2 (2017).; Brian L. Owlsey, "Network Investigative Source Code and Due Process," *Digital Evidence and Electronic Signature Law Review* 14 (2017).

25 David J. Bianco, "The Pyramid of Pain," 7 January 2014, http://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html.

7	Columbia network worm vaccine architecture experiment[vii]	June 2003	Vuln Reduction	Industry
8	Welchia / Nachi campaign targeting Blaster[viii]	August 2003	Vuln Reduction	Unknown
9	Netsky campaign targeting Beagle and MyDoom[ix]	February 2004	Criminal	Red-On-Red
10	Shadowcrew – Carderplanet underground marketplace takedown[x]	November 2004	Criminal	Gov (LE)
11	Welchia / Nachi-B campaign targeting MyDoom[xi]	November 2004	Vuln Reduction	Unknown
12	Harbin "QBTP worm" experiment[xii]	August 2005	Vuln Reduction	Industry
13	eGold takedown[xiii]	December 2005	Criminal	Gov (LE)
14	RBN bulletproof hosting takedown[xiv]	November 2007	Criminal	Industry
15	Kraken botnet exploitation[xv]	April 2008	Criminal	Industry
16	Darkmarket underground marketplace takedown[xvi]	October 2008	Criminal	PPP
17	McColo bulletproof hosting takedown[xvii]	November 2008	Criminal	Industry
18	Changsha "P2P anti-worm" experiment[xviii]	November 2008	Vuln Reduction	Industry
19	Srizbi takedown attempt[xix]	November 2008	Criminal	Industry
20	Storm botnet exploitation[xx]	December 2008	Criminal	Industry
21	Conficker botnet disruption[xxi]	November 2008 to June 2010	Criminal	PPP
22	Torpig botnet exploitation[xxii]	January – February 2009	Criminal	Industry
23	Ghostnet exploitation & disclosure[xxiii]	March 2009	Espionage	Industry
24	Simulated Bluetooth proximity malware white worm experiment[xxiv]	April 2009	Vuln Reduction	Industry
25	3FN bulletproof hosting takedown[xxv]	June 2009	Criminal	Gov (LE)
26	Algiers "father worm" experiment[xxvi]	July 2009	Benevolent	Industry
27	"Independence Day" botnet exploitation[xxvii]	July 2009	Strategic Attack	Industry
28	Mega-D botnet takedown[xxviii]	November 2009	Criminal	Industry
29	Lethic takedown attempt[xxix]	January 2010	Criminal	Industry
30	Waledec (b49) takedown[xxx]	February 2010	Criminal	Industry
31	Mariposa takedown[xxxi]	February 2010	Criminal	PPP
32	Troyak bulletproof hosting takedown[xxxii]	March 2010	Criminal	Industry

33	Dumps.name / BadB underground marketplace disruption[xxxiii]	August 2010	Criminal	Gov (LE)
34	Pushdo / Cutwail botnet takedown[xxxiv]	August 2010	Criminal	Industry
35	Bredolab takedown[xxxv]	October 2010	Criminal	PPP
36	Rustock (b107) takedown[xxxvi]	March 2011	Criminal	Industry
37	Coreflood takedown[xxxvii]	April 2011	Criminal	LE
38	DNSChanger takedown[xxxviii]	November 2011	Criminal	PPP
39	Ice IX possible exploitation[xxxix]	June 2012	Criminal	Industry
40	Grum botnet takedown[xl]	July 2012	Criminal	PPP
41	UGNazi takedown[xli]	May 2012	Hacktivist & Criminal	Gov (LE)
42	Syrian Electronic Army DarkComet possible exploitation[xlii]	November 2012 onward	Espionage	Unknown
43	Brobot takedown[xliii]	January 2013	Strategic Attack	Unknown
44	Dexter POS malware possible exploitation[xliv]	February 2013	Criminal	Industry
45	APT1 disclosure[xlv]	February 2013	Espionage	Industry
46	APT1 exploitation[xlvi]	March 2013	Espionage	Industry
47	Kelihos takedown attempt[xlvii]	March 2013	Criminal	Industry
48	Liberty Reserve takedown[xlviii]	May 2013	Criminal	Gov (LE)
49	Citadel (b54) takedown[xlix]	June 2013	Criminal	Industry
50	Carberp exploitation[l]	June 2013	Criminal	Red-On-Red
51	Blackhole Exploit Kit sales disruption[li]	October 2013	Criminal	Gov (LE)
52	Silk Road underground marketplace takedown[lii]	October 2013	Criminal	Gov (LE)
53	Zeroaccess disruption[liii]	December 2013	Criminal	PPP
54	Blackshades takedown[liv]	May 2014	Criminal	Gov (LE)
55	APT2 / PUTTER PANDA disclosure[lv]	May 2014	Espionage	Industry
56	GameOverZeus takedown[lvi]	June 2014	Criminal & Espionage	PPP
57	Shylock / Hijack takedown[lvii]	July 2014	Criminal	Gov (LE)
58	Citadel possible exploitation[lviii]	August 2014	Criminal	Industry
59	“Operation Onymous” underground marketplace takedowns[lix]	November 2014	Criminal	Gov (LE)

60	Asprox disruption[lx]	January 2015	Criminal	Gov (LE)
61	Ramnit takedown attempt[lxi]	February 2015	Criminal	Gov (LE)
62	SIMDA takedown[lxii]	April 2015	Criminal	PPP
63	Neverquest / Vawtrack takedown[lxiii]	April 2015	Criminal	PPP
64	Beebone takedown[lxiv]	April 2015	Criminal	Gov (LE)
65	APT30* / NAIKON / OVERRIDE PANDA* / LOTUS PANDA* disclosure[lxv]	July 2015	Espionage	Industry
66	Opfake exploitation[lxvi]	September 2015	Criminal	Industry
67	Dridex takedown[lxvii]	October 2015	Criminal	Gov (LE)
68	Dirt Jumper / Drive / Pandora possible exploitation[lxviii]	October 2015	Criminal	Industry
69	Dyre disruption[lxix]	November 2015	Criminal	Gov (LE)
70	Dorkbot takedown[lxx]	December 2015	Criminal	PPP
71	Lurk / Angler disruption[lxxi]	June 2016	Criminal	Gov (LE)
72	Hajime campaign[lxxii]	October 2016	Vuln Reduction	Unknown
73	Avalanche / KOL takedown[lxxiii]	November 2016	Criminal	PPP
74	Nymaim disruption[lxxiv]	December 2016	Criminal	PPP
75	Chanitor distribution of Vawtrack disruption[lxxv]	January 2017	Criminal	Gov (LE)
76	Cerber / Sage exploitation[lxxvi]	February 2017	Criminal	Industry
77	Blackmoon exploitation[lxxvii]	March 2017	Criminal	Industry
78	Neutrino bot exploitation[lxxviii]	March 2017	Criminal	Industry
79	Gaudox bot exploitation[lxxix]	March 2017	Criminal	Industry
80	Kelihos takedown[lxxx]	April 2017	Criminal	PPP
81	Brickerbot campaign[lxxxi]	April 2017	Vuln Reduction	Unknown
82	APT3 / GOTHIC PANDA / UPS TEAM disclosure[lxxxii]	May 2017	Espionage	Unknown
83	Plug-X possible exploitation[lxxxiii]	June 2017 onward	Espionage	Unknown
84	AlphaBay and Hansa underground marketplace takedowns[lxxxiv]	July 2017	Criminal	Gov (LE)
85	WireX disruption[lxxxv]	August 2017	Criminal	Industry
86	Andromeda botnet takedown[lxxxvi]	November 2017	Criminal	Gov (LE)

87	Mirai botnet disruption[lxxxvii]	March 2018	Hacktivist & Criminal	Gov (LE)
88	MaxiDed bulletproof hosting takedown[lxxxviii]	May 2018	Criminal	Gov (LE)
89	VPNFilter takedown[lxxxix]	May 2018	Espionage & Strategic Attack	PPP
90	MegaladonHTTP botnet possible exploitation[xc]	June 2018	Criminal	Industry
91	APT10 / STONE PANDA / MenuPass / POTASSIUM disclosure[xci]	August 2018	Espionage	Unknown
92	3ve takedown[xcii]	October 2018	Criminal	Gov (LE)
93	VPNFilter possible exploitation[xciii]	November 2019	Espionage & Strategic Attack	Unknown
94	Joanap takedown[xciv]	January 2019	Espionage & Strategic Attack	Gov (LE)
95	COBALT STRIKE abuse disclosure[xcv]	February 2019	Espionage & Criminal	Industry
96	Abdallah / Yalishanda hosting takedown[xcvi]	July 2019	Criminal	Gov (LE)
97	Retadup takedown[xcvii]	August 2019	Criminal	PPP
98	APT34 / HELIX KITTEN / OILRIG / COBALT GYPSY / CHRYSENE disclosure[xcviii]	April – May 2019	Espionage & Strategic Attack	Unknown
99	APT17 / AURORA PANDA / DOGFISH disclosure[xcix]	July 2019	Espionage	Unknown
100	CyberBunker bulletproof hosting takedown[c]	September 2019	Criminal	Gov (LE)
101	Turla / VENOMOUS BEAR / KRYPTON compromise of APT34 / OILRIG / CHRYSENE[ci]	November 2019	Espionage	Red-On-Red
102	H-Worm possible exploitation[cii]	November 2019	Espionage	Unknown
103	APT33 / REFINED KITTEN / COLBAT TRINITY infrastructure disclosure[ciii]	November 2019	Espionage	Industry

5. INITIAL INSIGHTS AND CONCLUSION

The debate over the appropriate approach, timing, and manner of actions intended to deny and degrade ongoing cyber threats closer to their origins has to date been a largely theoretical affair. The disconnects between policy communities and the operators and researchers engaged in the day-to-day fight on the wire have meant that in many cases, well-intentioned thinkers on both sides have been effectively talking past each other when discussing concepts of operation, desired end states,

and perceived drawbacks. While many key details of current and proposed future operations remain locked in classified discourse, the development of the framework proposed here, and the underlying dataset which has informed it, demonstrate that there is indeed a robust record of prior incidents by which to nominate courses of actions, illuminate conflicting equities, and advance reasoned arguments for both sides. Grounding ongoing conversations using a publicly documented dataset and the associated analytical features of these identified case studies will be useful in improving debates over differing policy and technical proposals.

Initial cross-case analysis already offers preliminary insights and clarifies questions to be further explored in depth for more robust testing and validation. Commonalities across the entirety of the case dataset importantly suggest that operational disruption is rarely accomplished as a single decisive action, at least where adversary operators, developers, and planners continue to enjoy a sustained base of uninterrupted support. However, merely because a single action will not render the adversary *hors de combat* does not negate the utility of disruption. Forcing adversary adaptation may add value, particularly where such a response requires investment disproportionate to the value of continuing operations or where adversary resourcing may be constrained in some other dimensions. Here the bias of the extant cases in the dataset must also be considered, where more technically effective options to achieve decisive results against adversary operations may have been available but precluded by the decision to pursue the operation under a law-enforcement framework, as opposed to national security or military authorities. From these cases, it appears that simpler direct-action options may have been available to disrupt adversary targets, but that more complex (as well as likely therefore more fragile) and higher-risk operations were conducted in order to preserve evidence for prosecution purposes, or to serve civil and coordination processes for later remediation of compromised victim systems. One may not presume that all future disruption efforts will be so constrained.

These potential issues have substantial relevance where targets are transnational criminal networks, especially those involved in both criminal activity and espionage operations, as a proxy on behalf of hostile intelligence services. In operational practice, one might note the case of the August 2019 Retadup takedown in light of these issues. During this law-enforcement action, pursued under European jurisdiction, disruption operators took steps to remove malware from compromised victim systems after successful takeover of botnet command & control infrastructure – measures that had been precluded in a number of previous campaigns conducted under other jurisdictions for fear of liability exposure, or due to ethical concerns.[26]

26 Felix Leder, Tillmann Werner, and Peter Martini, "Proactive Botnet Countermeasures – An Offensive Approach," in *The Virtual Battlefield: Perspectives on Cyber Warfare*, ed. Christian Czosseck and Kenneth Geers. IOS Press, 2009.; David Dittrich, Felix Leder, and Tillmann Werner, "A Case Study in Ethical Decision Making Regarding Remote Mitigation of Botnets," *International Conference on Financial Cryptography and Data Security. Tenerife, Canary Islands, Spain, 25-28 January 2010*.; Sam Zeitlin, "Botnet Takedowns and the Fourth Amendment," *New York University Law Review* 90, no. 2 (May 2015): 746-778.

Disruptions made for vulnerability reduction, such as the CodeRed / CodeGreen case study, are important transitional actions, often taken by defense-minded actors who have expressed frustration at unmitigated exposure or ongoing adversary action that has apparently gone unaddressed – and including what are believed to be the earliest documented hackback actions by non-state actors. These cases serve as an instructive contrast to more structured and deliberate operations as they are typically unilateral, with uncoordinated execution and significant potential for collateral damage and escalation. Experimentation with purely technical capabilities, they may have informed later concepts of operation by other actors acting within different constraints, where technical options are modified to meet acceptable criteria defined by political, judicial, or operational oversight.

Red-on-red cases surface with particular salience where state intelligence services – in an attempt to advance deception themes or achieve surprise – leverage criminal capabilities acquired through transactional engagements, or coercive leverage, to intertwine espionage and strategic attack objectives with criminal operations. Where such capabilities are co-mingled, the state service involved takes on a greater operational risk, as criminal infrastructure is more commonly targeted by other criminals who share common understanding of tactics, techniques, and procedures and are aware of routine failures in operational practice that may lead to takeover or competitive disruption. Yet at the same time, these cases perhaps suggest that escalation concerns over adversary reaction to disruptive operations may be lessened in a number of situations, given prior incidents in which state actors leveraging co-mingled infrastructure apparently did not respond directly. Nonetheless, the small number of documented incidents demands further cautious consideration beyond such tentative, preliminary insight.

We hope this framework and dataset bring transparency and repeatability to the critical issue of disruptive counter-cyber operations. Future research in this area – both by academics and practitioners in the government or commercial cyber threat intelligence field – should improve our framework, apply it to the full data set to allow deeper insights, and develop additional case studies. A student capstone project at Columbia University's School of International and Public Affairs is specifically researching the impact on adversaries of one specific kind of disruption, public disclosure.

The dataset published here does demonstrate that, far from an unprecedented break with past practice, new proposed disruption approaches may be considered evolutionary in design and execution and may be evaluated within a common framework. Lessons from prior disruptive actions can improve future operations by the US government, its allies, and other likeminded actors – especially given reported intentions to pursue more assertive employment of offensive measures for counter-cyber operations within

the context of the persistent engagement framework, implementing the strategic vision of "defend forward". These cases help to understand the likely upper bounds of such operations, and how such actions may be tailored to cause the most friction under differing situations. It is believed that a neutral, objective analytic construct is the best mechanism for evaluating comparative countering options, with the hope that it will focus planning and action in a manner that denies and degrades adversary capabilities at the greatest scale, the least cost, and with the lowest chance of escalation.

APPENDIX: REFERENCES FOR TABLE 1, DATASET OF CYBER DISRUPTION EVENTS

i Capek, Peter G., David M. Chess, Steve R. White, and Alan Fedeli. "Merry Christma: An Early Network Worm." *IEEE Security & Privacy* 1, no. 5 (Sept.–Oct. 2003): 26-34.

ii Skulason, Fridrik. "The Search for Den Zuk." *Virus Bulletin*. February 1991.

iii Barber, Bryan. "Cheese Worm: Pros and Cons of a Friendly Worm." SANS Institute. 26 July 2001.

iv Der HexXer, Herbert. "CodeGreen Beta Release." *Vuln-Dev*. 1 September 2001.

v Metzer, David J. "The Coming Age of Defensive Worms." *Toorcon*. September 2003.

vi Symantec. "W32.Klez.A@mm." 25 October 2001.

vii Sidiroglou, Stelios, Angelos D. Keromytis. "A Network Worm Vaccine Architecture." *Proceedings of the 12th IEEE International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE). Linz, Austria. 11-11 June 2003*.

viii Symantec. "W32.Welchia.Worm." 18 August 2003.

ix Edwards, Dwayne. "Netsky.p Mass Mailer Worm Analysis." *SANS Institute*. 9 January 2005.

x DOJ. "Nineteen Individuals Indicted in Internet 'Carding' Conspiracy: Shadowcrew Organization Called 'One-Stop Online Marketplace for Identity Theft."" 28 October 2004. https://www.justice.gov/archive/criminal/cybercrime/press-releases/2004/mantovaniIndict.htm; James Verini. "The Great Cyberheist." *The New York Times Magazine*. 10 November 2010.; DOJ. "Ukrainian National Who Co-Founded Cybercrime Marketplace Sentenced To 18 Years in Prison." 12 December 2013, https://www.justice.gov/usao-edny/pr/ukrainian-national-who-co-founded-cybercrime-marketplace-sentenced-18-years-prison.

xi Symantec. "W32.Welchia.B.Worm." 18 November 2004.

xii Liu, Yi-Xuan, Xiao-Chun Yun, Bai-Ling Wang, Hai-Bin Sun. "QBTP Worm: An Anti-Worm with Balanced Tree Based Spreading Strategy." *Proceedings of the Fourth International Conference on Machine Learning and Cybernetics. Guangzhou, People's Republic of China. 18-21 August 2005*.

xiii Zetter, Kim. "Bullion and Bandits: The Improbable Rise and Fall of E-Gold." Wired. 9 June 2009.

xiv iDefense. "The Russian Business Network: Rise and Fall of a Criminal ISP." 3 March 2008.

xv Mushtaq, Atif. "Kraken Botnet – A Detailed Analysis." *FireEye*. 17 April 2008, https://www.fireeye.com/blog/threat-research/2008/04/kraken-botnet-1.html.

xvi Alperovitch, Dmitri and Keith Mularski. "Fighting Russian Cybercrime Mobsters: Report from the Trenches." *Black Hat USA. Las Vegas, Nevada. 29-30 July 2009*.

xvii Krebs, Brian. "Host of Internet Spam Groups Is Cut Off." *Washington Post*. 12 November 2008.

xviii Wang, Bin, Piao Ding, Jinfang Sheng. "P2P Anti-worm: Modeling and Analysis of a New Worm Counter-measurement Strategy." *9th International Conference for Young Computer Scientists. Hunan, People's Republic of China. 18-21 November 2008*.

xix Keizer, Gregg. "Massive Botnet Returns From The Dead, Starts Spamming." Computerworld. 26 November 2008.

xx Wicherski, Georg 'oxff', Tillmann Werner, Felix Leder, Mark Schlösser. "Stormfucker: Owning the Storm Botnet." *25th Chaos Communication Congress. Berlin, Germany. 29 December 2008*.

xxi Rendon Group. "Conficker Working Group: Lessons Learned." January 2011.

xxii Stone-Gross, Brett, Marco Cova, Lorenzo Cavallaro, Bob Gilbert, Martin Szydlowski, Richard Kemmerer, Christopher Kruegel, Giovanni Vigna. "Your Botnet is my Botnet: Analysis of a Botnet Takeover." *16th ACM conference on Computer and communications security (CCS). Chicago, Illinois. 9-13 October 2009*.

xxiii Information Warfare Monitor. "Tracking GhostNet: Investigating a Cyber Espionage Network." 29 March 2009.

xxiv Zyba, Gjergji, Geoffrey M. Voelker, Michael Liljenstam, Andras Mehes, Per Johansson. "Defending Mobile Phones from Proximity Malware." *IEEE INFOCOM. Rio de Janeiro, Brazil. 19-25 April 2009*.

xxv Krebs, Brian. "FTC Sues, Shuts Down N. Calif. Web Hosting Firm." *Washington Post*. 4 June 2009.

xxvi Berbar, Ahmed, Mohamed Ahmednacer. "Testing and Fault Tolerance Approach for Distributed Software Systems Using Nematode Worms." *Proceedings of the 4th International Conference on Queueing Theory and Network Applications (QTNA). July 2009*.

xxvii iSIGHT Partners. "Peer-to-Peer Command-and-Control Architecture Likely Used in Sustained DDoS Attacks Against South Korean and U.S. Targets." 9 July 2009.; Nguyen, Minh Duc. "Comments on Korea and US DDOS Attacks." *BKIS*. 14 July 2009, http://blog.bkis.com/?p=718.

xxviii Lin, Phillip. "Anatomy of the Mega-D takedown." Network Security. (December 2009): 4-7.; Cho, Chia Yuan, Juan Caballero, Chris Grier, Vern Paxson, and Dawn Song. "Insights from the Inside: A View of Botnet Management from Infiltration." *3rd Usenix Workshop on Large Scale Exploits and Emergent Threats (LEET). San Jose, CA. 28-30 April 2010*.

xxix Zscaler. "Lethic Botnet Returns, Uses "Realtek" Identifier." 10 November 2010.

xxx Cranton, Tim. "Cracking Down on Botnets." *Microsoft*. 24 February 2010, https://blogs.technet.microsoft.com/microsoft_on_the_issues/2010/02/24/cracking-down-on-botnets/.

xxxi Sully, Matt, and Matt Thompson. "The Deconstruction of the Mariposa Botnet." *Defence Intelligence.* February 2010.

xxxii McMillan, Robert. "Zeus Botnet Dealt a Blow as ISP Troyak Knocked Out." *Computerworld*. 10 March 2010; McMillan, Robert. "After Takedown, Botnet-Linked ISP Troyak Resurfaces." *Computerworld*. 10 March 2010.

xxxiii DOJ. "Alleged International Credit Card Trafficker Arrested in France on U.S. Charges Related to Sale of Stolen Card Data." 11 August 2010, https://www.justice.gov/opa/pr/alleged-international-credit-card-trafficker-arrested-france-us-charges-related-sale-stolen.

xxxiv iSIGHT Partners. "Potential 'Dead Hand' C&C Architecture Suggested by Adversary Adaptation Following Failed Botnet Takedown Attempt." 11 February 2010.; JD Work. "Autonomy & Conflict Management in Offensive & Defensive Cyber Engagement." *IWCon. Nashville, TN. 5-7 April 2016*.

xxxv Williams, Jeff. "Bredolab Takedown, Another Win for Collaboration." *Microsoft*. 26 October 2010. http://blogs.technet.com/b/mmpc/archive/2010/10/26/bredolabtakedown-another-win-for-collaboration.aspx.

xxxvi Boscovich, Richard. "Taking Down Botnets: Microsoft and the Rustock Botnet." *Microsoft*. 17 March 2011, https://blogs.technet.microsoft.com/microsoft_on_the_issues/2011/03/17/taking-down-botnets-microsoft-and-the-rustock-botnet/.

xxxvii DOJ. "Department of Justice Takes Action to Disable International Botnet." 13 April 2011, https://www.justice.gov/opa/pr/department-justice-takes-action-disable-international-botnet.

xxxviii Trend Micro. "OPERATION GHOST CLICK: The Rove Digital Takedown." 2012.

xxxix Sood, Aditya K. "For Fun - XSS in ICE IX C&C Panel." 12 June 2012, https://secniche.blogspot.com/2012/06/for-fun-xss-in-ice-ix-bot-admin-panel.html.

xl Mushtaq, Atif. "Grum, World's Third-Largest Botnet, Knocked Down." *FireEye*. 18 July 2012.

xli Honan, Mat. "Cosmo, the Hacker 'God' Who Fell to Earth." *Wired*. 11 September 2012.

xlii Denbow, Shawn and Jesse Hertz. "Pest Control: Taming the Rats." *Matasano Security*. October 2012.

xliii Work, JD. "Echoes of Ababil: Re-Examining Formative History of Cyber Conflict and its Implications for Future Engagements." *Society of Military History Annual Conference. Cincinnati, OH. 9-12 May 2019*.

xliv Wallace, Brian. "A Study in Bots: Dexter." *Cylance*. 14 March 2014, https://threatvector.cylance.com/en_us/home/a-study-in-bots-dexter-pos-botnet-malware.html.

xlv Mandiant. "APT1: Exposing One of China's Cyber Espionage Units." 19 February 2013, https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf.

xlvi Rascagnères, Paul. "APT1: Technical Backstage." *Malware.lu*. 27 March 2013.

xlvii Werner, Tillmann. "Peer-to-Peer Poisoning Attack against the Kelihos.C Botnet." *CrowdStrike*. 21 March 2013.

xlviii DOJ. "Manhattan U.S. Attorney Announces Charges Against Liberty Reserve, One of World's Largest Digital Currency Companies, and Seven of its Principals and Employees for Allegedly Running a $6 Billion Money Laundering Scheme." 28 May 2013, https://www.justice.gov/usao-sdny/pr/manhattan-us-attorney-announces-charges-against-liberty-reserve-one-world-s-largest.

xlix Meisner, Jeffrey. "Microsoft Works with Financial Services Industry Leaders, Law Enforcement and Others to Disrupt Massive Financial Cybercrime Ring." *Microsoft*. 5 June 2013.

l Steven K. “Carberp Remote Code Execution: Carpwned.” XyliBox blog. 28 June 2013, https://www.xylibox.com/2013/06/carberp-remote-code-execution-carpwned.html.

li FireEye. “Black Hole Exploit Kit: The Rise and Fall of an Exploit Kit Giant.” 28 March 2014.

lii Zetter, Kim. “How the Feds Took Down the Silk Road Drug Wonderland.” *Wired*. 18 November 2013, https://www.wired.com/2013/11/silk-road/.

liii Microsoft. “Microsoft, the FBI, Europol and Industry Partners Disrupt the Notorious ZeroAccess Botnet.” 5 December 2013, https://news.microsoft.com/2013/12/05/microsoft-the-fbi-europol-and-industry-partners-disrupt-the-notorious-zeroaccess-botnet/.

liv FBI. “International Blackshades Malware Takedown Coordinated Law Enforcement Actions Announced.” 19 May 2014, https://www.fbi.gov/news/stories/international-blackshades-malware-takedown-1.

lv CrowdStrike. “Putter Panda.” May 2014.

lvi DOJ. “U.S. Leads Multi-National Action Against ‘Gameover Zeus’ Botnet and ‘Cryptolocker’ Ransomware, Charges Botnet Administrator.” 2 June 2014, https://www.justice.gov/opa/pr/us-leads-multi-national-action-against-gameover-zeus-botnet-and-cryptolocker-ransomware.

lvii Europol. “Global Action Targeting Shylock Malware.” 10 July 2014, https://www.europol.europa.eu/newsroom/news/global-action-targeting-shylock-malware.

lviii Sood, Aditya K. “Exploiting Fundamental Weaknesses in Botnet Command and Control Panels.” *Black Hat. Las Vegas, NV. 2-7 August 2014*.

lix Europol. “Global Action Against Dark Markets on Tor Network.” 7 November 2014, https://ec.europa.eu/home-affairs/what-is-new/news/news/2014/20141107_01_en.

lx Secureworks. “Evolution of the GOLD EVERGREEN Threat Group.” 15 May 2017.

lxi Europol. “Botnet Taken Down Through International Law Enforcement Cooperation”. 25 February 2015. https://www.europol.europa.eu/newsroom/news/botnet-taken-down-through-international-law-enforcement-cooperation; Symantec. “Ramnit Cybercrime Group Hit by Major Law Enforcement Operation.” 25 February 2015.; Trend Micro. “Ramnit: The Comeback Story of 2016.” 20 February 2017.

lxii Interpol. “INTERPOL Coordinates Global Operation to Take Down Simda Botnet.” 13 April 2015, https://www.interpol.int/en/News-and-Events/News/2015/INTERPOL-coordinates-global-operation-to-take-down-Simda-botnet.

lxiii Takada, Kazuki. “Behind Operation Banking Malware Takedown and the Progression of Malware Sophistication.” *Code Blue. Tokyo, Japan. 20-21 October 2016*.

lxiv Europol. “International Police Operation Targets Polymorphic Beebone Botnet.” 9 April 2015, https://www.europol.europa.eu/newsroom/news/international-police-operation-targets-polymorphic-beebone-botnet.

lxv FireEye. “APT 30 and the Mechanics of a Long-Running Cyber Espionage Operation.” 12 April 2015.; ThreatConnect. “Project CameraShy: Closing the Aperture on China’s Unit 78020.” July 2015.

lxvi Huang, Wayne and Sun Huang. “24 Techniques to Gather Threat Intel and Track Actors.” *Black Hat Asia. Singapore. 28-31 March 2017*.

lxvii Secureworks. “Dridex (Bugat v5) Botnet Takeover Operation.” 13 October 2015.

lxviii Watkins, Lanier, Kurt Silberberg, Jose Andre Morales, William H. Robinson. “Using Inherent Command and Control Vulnerabilities to Halt DDoS Attacks.” *10th International Conference on Malicious and Unwanted Software. Fajardo, Puerto Rico. 20–22 October 2015*.

lxix Symantec. “Dyre: Operations of Bank Fraud Group Grind to Halt Following Takedown.” 8 February 2016.

lxx Interpol. “INTERPOL Supports Global Operation Against Dorkbot Botnet.” 4 December 2015.

lxxi Biasini, Nick. “Connecting the Dots Reveals Crimeware Shake-up.” *Cisco TALOS*. 7 July 2016.

lxxii Grange, Waylon. “Hajime Worm Battles Mirai for Control of the Internet of Things.” *Symantec*. 18 April 2017.; Yamaguchi, Shingo, Pattara Leelaprute. “Hajime Worm with Lifespan and Its Mitigation Evaluation Against Mirai Malware Based on Agent-Oriented Petri Net PN2.” *IEEE International Conference on Consumer Electronics (ICCE). Las Vegas, NV 11–13 January 2019*.

lxxiii Europol. “Avalanche Network Dismantled in International Cyber Operation.” 1 December 2016, https://www.europol.europa.eu/newsroom/news/%E2%80%98avalanche%E2%80%99-network-dismantled-in-international-cyber-operation.

lxxiv CrowdStrike. “Goznym: Gozi Malware Hybrid Bundled with the Nymaim Loader.” 2 June 2017.

lxxv FireEye. “Operational Net Assessment for Cyber Crime: January to March 2017.” 4 April 2017.

lxxvi Huang and Huang, 2017.

lxxvii Huang and Huang, 2017.

lxxviii Huang and Huang, 2017.

lxxix Huang and Huang, 2017.

lxxx CrowdStrike. “Inside the Takedown of ZOMBIE SPIDER and the Kelihos Botnet.” 13 April 2017.

lxxxi DHS CISA. “BrickerBot Permanent Denial-of-Service Attack.” 12 April 2017, https://www.us-cert.gov/ics/alerts/ICS-ALERT-17-102-01A.

lxxxii Recorded Future. “Recorded Future Research Concludes Chinese Ministry of State Security Behind APT3.” 17 May 2017.; Checkpoint. “UPSynergy: Chinese-American Spy vs. Spy Story.” 5 September 2019.

lxxxiii Grange, Waylon. “Digital Vengeance: Exploiting the Most Notorious C&C Toolkits.” *Black Hat. Las Vegas, NV. 22–27 July 2017*.

lxxxiv Europol. “Massive Blow to Criminal Dark Web Activities After Globally Coordinated Operation.” 20 July 2017, https://www.europol.europa.eu/newsroom/news/massive-blow-to-criminal-dark-web-activities-after-globally-coordinated-operation.

lxxxv Grooten, Martijn. “WireX DDoS Botnet Takedown Shows the Best Side of the Security Industry.” *Virus Bulletin*. 29 August 2017.

lxxxvi Europol. “Andromeda Botnet Dismantled in International Cyber Operation.” 4 December 2017, http://www.eurojust.europa.eu/press/PressReleases/Pages/2017/2017-12-04.aspx.

lxxxvii Graff, Garrett M. “The Mirai Botnet Architects Are Now Fighting Crime With the FBI.” *Wired*. 18 September 2018.

lxxxviii Noroozian, Arman, Eelco van Veldhuizen, Carlos H. Ganan, Sumayah Alrwais, Damon McCoy, Michel van Eeten. “Platforms in Everything: Analyzing Ground-Truth Data on the Anatomy and Economics of Bullet-Proof Hosting.” *28th Usenix Security Symposium. Santa Clara, CA. 14–16 August 2019*.

lxxxix DOJ. “Justice Department Announces Actions to Disrupt Advanced Persistent Threat 28 Botnet of Infected Routers and Network Storage Devices.” 23 May 2018, https://www.justice.gov/opa/pr/justice-department-announces-actions-disrupt-advanced-persistent-threat-28-botnet-infected.

xc Nachum, Shay, Assaf Schuster, Opher Etzion. “Detection in the Dark – Exploiting XSS Vulnerability in C&C Panels to Detect Malwares.” *Cyber Security Cryptography and Machine Learning (CSCML). Beer Sheva, Israel. 21-22 June 2018*.

xci FireEye. “Assessment of Recent Public Reports Regarding APT10.” 8 August 2019.

xcii DHS CISA. “3ve – Major Online Ad Fraud Operation.” 27 November 2018, https://www.us-cert.gov/ncas/alerts/TA18-331A.

xciii Olney, Matthew. “Seeing Broad Scanning...” *Twitter*. 27 November 2018, https://twitter.com/kpyke/status/1068141372543242240.

xciv DOJ. “Justice Department Announces Court-Authorized Efforts to Map and Disrupt Botnet Used by North Korean Hackers.” 30 January 2019, https://www.justice.gov/opa/pr/justice-department-announces-court-authorized-efforts-map-and-disrupt-botnet-used-north.

xcv Strategic Cyber, LLC. “Cobalt Strike Team Server Population Study.” 19 February 2019. https://blog.cobaltstrike.com/2019/02/19/cobalt-strike-team-server-population-study/; Work, JD. “In Wolf’s Clothing: Complications of Threat Emulation in Contemporary Cyber Intelligence Practice.” *Cyber Incident. University of Oxford, 3-4 June 2019*.

xcvi Krebs, Brian. “Meet the World’s Biggest ‘Bulletproof’ Hoster.” *Krebs on Security*. 16 July 2019. https://krebsonsecurity.com/2019/07/meet-the-worlds-biggest-bulletproof-hoster/; Security Service of Ukraine. “SBU Jointly with Foreign Colleagues Blocks Activity of Powerful Hacker Group.” 16 July 2019, https://ssu.gov.ua/en/news/1/category/21/view/6281#.J1jZcicu.dpbs.

xcvii Vojtěšek, Jan. “Putting an End to Retadup: A Malicious Worm that Infected Hundreds of Thousands.” *Avast*. 28 August 2019, https://decoded.avast.io/janvojtesek/putting-an-end-to-retadup-a-malicious-worm-that-infected-hundreds-of-thousands/.

xcviii FireEye. “Leaking Campaigns Designed to Degrade Iranian Cyber Capabilities Continue.” 11 June 2019.

xcix FireEye. “APT17 Outed as MSS Operation.” 25 July 2019.

c Krebs, Brian. “German Cops Raid “Cyberbunker 2.0,” Arrest 7 in Child Porn, Dark Web Market Sting.” *Krebs on Security*. 28 September 2019, https://krebsonsecurity.com/2019/09/german-cops-raid-cyberbunker-2-0-arrest-7-in-child-porn-dark-web-market-sting/.

ci National Security Agency and National Cyber Security Center. “Turla Group Exploits Iranian APT to Expand Coverage of Victims.” 21 October 2019, https://www.ncsc.gov.uk/news/turla-group-exploits-iran-apt-to-expand-coverage-of-victims.

cii Reporting by the self-styled “Democratic People’s Republic of Korea Computer Emergency Response Team (CERT).” “Vulnerability in the Remote Administration Tool (RAT) H-Worm.” 6 November 2019.

ciii Hacquebord, Feike, Cedric Pernet, and Kenney Lu. “More than a Dozen Obfuscated APT33 Botnets Used for Extreme Narrow Targeting.” *Trend Micro*. 13 November 2019, https://blog.trendmicro.com/trendlabs-security-intelligence/more-than-a-dozen-obfuscated-apt33-botnets-used-for-extreme-narrow-targeting/.