CyberPeace
Institute

Case Study:
WreckWeb

This case study helps showcase how the CyberPeace Institute would operate in response to and in the aftermath of a global cyber event called “WreckWeb.”

The fictional ransomware attack is based on multiple real world examples and allows this case study to highlight how each of the Institute’s functions would be expected to react when fully operational.

The case study has four sections:

I. Anatomy of a global cyber incident – NotPetya
II. CyberPeace Institute Function: Assistance
III. CyberPeace Institute Function: Accountability
IV. CyberPeace Institute Function: Advancement

Recent years have seen a significant increase in the frequency and impact of sophisticated cyberattacks. Major incidents like the NotPetya, WannaCry, Triton, and Shamoon cyberattacks have become household names, hacking incidents at organizations like Equifax and Sony Pictures have grabbed headlines, and lesser known ransomware attacks continue to regularly paralyze businesses and municipalities around the world. This report begins by exploring the anatomy and impact of one highly prominent example – the 2017 NotPetya attack. This attack, which originated in Ukraine and spread to infect computer systems around the world, is a seminal event in the history of cyber tensions. In addition to capturing the impact and scale of the attack, this opening section also presents some of the gaps in the international response that existed at the time of the NotPetya attack and which the CyberPeace Institute will seek to address.

The subsequent sections of the report then illustrate how each of the Institute’s functions would, in turn, be activated and respond in the wake of a similar incident today, a ransomware attack we have called “WreckWeb.” These sections bring the work of the Institute to life at the individual level. They tell the story of how a humanitarian NGO seeks and receives emergency assistance from the Institute when they are compromised by WreckWeb, how technical and impact analyses are coordinated by the Institute to capture the nature of the attack and the damage it caused, and how information about the attack is shared with the world to inform discussions about how to reduce the risk of such events in the future.

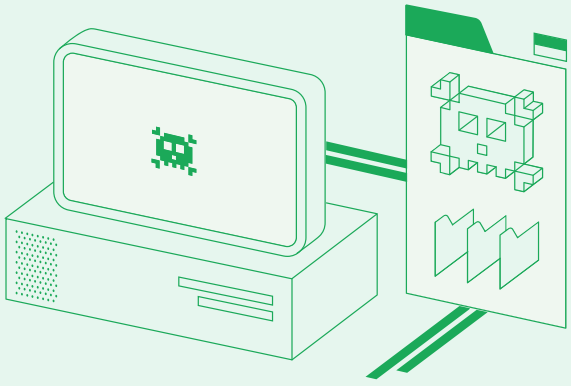
For the purposes of this report, there are presumptions made about how particular individuals and organizations might engage with the work of the CyberPeace Institute. This is purely to be illustrative of how the Institute would operate and is not meant to reflect actual commitments or obligations by third parties. Ultimately, the case study provides exemplary context for how we envision the CyberPeace Institute would partner with others, operate efficiently and effectively, and add unique value to the ecosystem going forward.

Contents

Anatomy of a global cyber incident – **NotPetya**

The summer of 2017 brought with it one of the most damaging cyberattacks in history. We use it at the outset of this case study to demonstrate the real world impacts that cyberattacks can have, but move on later in the document to weaving a completely fictional narrative.

The NotPetya attack was selected as it showed what was possible when cyberweapons developed by sophisticated actors are used indiscriminately and without consideration for consequence, and highlights the need for greater action to curb the dangers of these attacks in the future.



Overview of the Attack

The early morning hours of an otherwise calm summer Tuesday, on June 27th, 2017, stood as silent witness to the onslaught of NotPetya, a precedent-shattering cyberattack. The sophisticated malware was first deployed via tax software used ubiquitously throughout Ukraine, with initial infections targeting the computers of an electric company.[1] But within hours of the initial outbreak, organizations from finance, transportation, energy, commercial, and healthcare sectors around the world stood paralyzed.[2] Computers were suddenly rendered useless; their benefit to society reduced to little more than expensive paperweights. Tens of thousands of machines across the globe were brought down in a matter of hours by one of the most insidious viral infections since the Spanish flu pandemic of 1918.[3]

At first, NotPetya presented itself as highly derivative, even familiar, ransomware. It combined the powerful encryption methods of earlier attacks, collectively referred to as "Petya," with a terrifying virality effected through use of a once-secret government-developed tool called "EternalBlue." Stolen and later leaked on the web, EternalBlue had already allowed the WannaCry ransomware to spread autonomously through file-sharing networks just a month earlier.

Tens of thousands of machines across the globe were brought down in a matter of hours

However, unlike its digital predecessors, such as WannaCry, the NotPetya attack was not ransomware at all. Despite appearing like ransomware, NotPetya actually functioned as a weapon, intent on permanently sabotaging targeted computer systems to sow chaos online and off.[4] Its victims were diverse, from families to firms, as the virus went to work overwriting dreams, memories, and the lifeblood of companies in a whirl of transcendent destruction.[5]

[1] https://www.tripwire.com/state-of-security/security-data-protection/cyber-security/notpetya-timeline-of-a-ransomworm/

[2] https://www.us-cert.gov/ncas/alerts/TA17-181A

[3] https://www.zdnet.com/article/petya-ransomware-attack-how-many-victims-are-there-really/

[4] https://www.theregister.co.uk/2017/06/28/petya_notpetya_ransomware/

[5] https://securelist.com/expetrpetyanotpetya-is-a-wiper-not-ransomware/78902/

Impacts of the attack

Disguising itself as ransomware, NotPetya immediately locked users out of their infected systems by overwriting the master boot record and encrypting the master file table to make data unreachable, A user screen demanded $300 in bitcoin in exchange for a decryption key.[6] The ransomware façade quickly faded, however, when it became clear that the destructive worm had made it impossible to decrypt data. Moreover, shortly after the attack began, the email address that provided the only link to the attackers went dead.

While the attack did not have a financial motive, NotPetya did result in significant financial costs – totaling more than $10 billion, according to figures provided by the White House. The attack originated in, and appeared to target, Ukraine – where approximately 80% of the infections took place – but it quickly spread and inflicted significant damage on organizations across the globe, crippling shipping giants, major transportation and food companies, government agencies, and a host of smaller businesses.[7] Moreover, the intangible costs of the NotPetya attack, including disrupted access to critical services, are more difficult to capture and calculate, but nonetheless imposed a terrible toll on victims as well.

[6] https://www.csoonline.com/article/3233210/petya-ransomware-and-notpetya-malware-what-you-need-to-know-now.html

[7] https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

Dealing with NotPetya

Unlike the ransomware attacks it mimicked, the damage of NotPetya was never designed to be undone. Soon after the initial reported cases, it became clear that there was no "kill switch", as there had been in the WannaCry attack a month earlier. Simply put, there was no way for victims (or even the attackers themselves) to fully restore compromised systems. Instead, the response to NotPetya is a story of triage – managing a crisis to limit damage and often simply accepting significant and permanent loss. Thankfully, because the methods employed in NotPetya mirrored those of earlier attacks, there were already fixes in place to defend against much of the autonomous spread of the attack – if users had taken the time to apply them in advance.[8]

These solutions included patches for the vulnerabilities in the Windows operating system that NotPetya exploited. For fully supported software, the patch needed to prevent the primary method by which NotPetya spread across networks – the EternalBlue exploit[9] – was released by Microsoft several months before the attack, on March 14, 2017.[10] Moreover, even older software that was no longer supported, such as Windows XP, had an emergency patch made available to address the vulnerability following the WannaCry attack the previous month, on May 12th, which had relied on the same stolen exploit.[11]

However, organizations that had not taken time to update their systems were left vulnerable to infection and the spread of NotPetya's wiper software across their networks. As a result, response efforts frequently involved teams working to isolate the virus and secure uninfected machines. Many organizations and individuals hit by NotPetya utilized commercial incident response services to contain the attack, recover data, and learn what policies or practices they could employ to help prevent future attacks. Other affected organizations and victimized individuals, however, were unable to afford such services, or indeed know where to look for help.

[8] https://www.csoonline.com/article/3233210/petya-ransomware-and-notpetya-malware-what-you-need-to-know-now.html

[9] "Exploit" in this context refers to code that takes advantage of a flaw in computer hardware or software to enable unintended and/or malicious effects.

[10] https://www.us-cert.gov/ncas/alerts/TA17-181A

[11] https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/

Many experts initially suspected a state actor bore responsibility for NotPetya given how the attack began, spreading through Ukrainian tax software and targeting critical sectors in Ukraine on the eve of a national holiday. They viewed NotPetya as part of a larger, ongoing effort to undermine and destabilize the Ukrainian state. Further forensic work by security researchers noted that the attack appeared to be the work of the same groups that were responsible for the December 2016 attacks against Ukrainian critical infrastructure.[12]

In February of 2018, seven governments – Australia, Estonia, Denmark, Lithuania, Ukraine, the United Kingdom and the United States – each issued respective statements formally attributing the attack to Russia and the Russian military. This attribution was not, however, accompanied by any significant public evidence of their responsibility, nor was there a meaningful effort to assess the NotPetya attack as a violation of any existing international laws or norms.[13] Indeed, it is not clear how these seven governments—or others—understood the relevant legal frameworks. Did NotPetya's Ukrainian targeting implicate the laws of armed conflict or did its global impacts warrant evaluation under other international legal frameworks, like the duty of non-intervention and human rights, not to mention the voluntary norms of responsible state behavior adopted by a UN Group of Government experts in 2015? For its part, Russia subsequently denied any responsibility for the attack. Indeed, the government cited evidence that several Russian organizations had even been harmed by NotPetya as well.

Looking backward from today, we wonder how the existence of the CyberPeace Institute might respond and change the course of events in the wake of similar cyber incidents. How might it limit the harm to civilian victims? Promote accountability for the damage that was caused? And advance the development and enforcement of rules to protect cyberspace from such wanton and indiscriminate attacks?

[12] https://ssu.gov.ua/ua/news/1/category/2/view/3660#.FeY6y8di.dpbs
[13] https://www.cfr.org/interactive/cyber-operations/notpetya

The following sections of this case study outline how the CyberPeace Institute would respond to a fictional global cyber incident, based on various examples including NotPetya, called WreckWeb, and its aftermath. The persons and events described below are fictitious but illustrative of the real potential value of the Institute. In the anecdotes that follow there lives a detailed description of the Institute's three core functions – Assistance, Accountability and Advancement – and how they might operate in a crisis of the size, speed, and scale of the NotPetya attack. It chronicles the work of a handful of full-time employees and a globe-spanning network of volunteers; the leading edge in a new era in cybersecurity; the stories of the men and women of the CyberPeace Institute.

CyberPeace Institute Function: **Assistance**

In the immediate aftermath of a sophisticated ransomware attack called WreckWeb, the CyberPeace Institute's Assistance function focuses on leveraging partnerships and resources to assist civilian victims in recovering from the attack and preventing future incidents.

Engaging the CyberVolunteer Network

On an otherwise calm morning in early October, the humanitarian assistance organization HappyHelpers International wakes to find several of its relief missions, in Syria as well as Lebanon, infected by the WreckWeb virus, a sophisticated ransomware attack that had started spreading rapidly across Europe just the day before. As a nongovernmental organization chartered in London, HappyHelpers has worked for more than 18 months to deliver immediate aid to civilians trapped by an endless civil war inside the ruins of Syria, as well as to those who had escaped the conflict and live as refugees abroad.

At HappyHelpers' burgeoning hub in the Turkish border town of Reyhanli, the scene is tense. Computers are locked and unusable, their contents encrypted while a black screen with white letters explains that restoring files is only possible with a decryption key in exchange for a ransom payment in a cryptocurrency that those on site hadn't even heard of previously. Aid workers scramble to activate disused satellite phones and international cellular calling plans, desperate to warn partners in the Syrian diaspora. Not knowing who is behind the attack, HappyHelpers workers look to warn their countrymen that personnel data in their systems may no longer be secret from the Syrian regime's death squads. These same workers, meanwhile, cannot access time critical information about food shipments and water purification processes. They are reduced to waiting and watching, with a front-row seat to a growing global crisis.[14]

[14] While this scenario is fictitious, numerous NGOs are regularly affected by ransomware and other cyberattacks and struggle to continue operations; e.g., a small nonprofit providing cancer services was affected by ransomware, which not only disrupted services but also made it difficult to apply for grant funding. https://www.npr.org/2017/05/20/529257365/small-indiana-nonprofit-falls-victim-to-ransom-cyberattack

Facing an existential threat to her organization's ability to function, Fatima Khourari, the Regional Assistance Director for HappyHelpers, makes a call to a well-known contact at a Turkish law firm specializing in humanitarian relief. The call connects and Khourari's words come tumbling out in a rush: the NGO is working to try and deliver fresh water and food to refugees in one of the newly announced "safe zones" around Idlib during a brief lull in the fighting. The apparent ransomware attacks have paralyzed the NGO and blocked access to the email and spreadsheets needed to track trucks carrying the aid as they make the perilous journey through Turkey and across a deeply mistrustful border. Time is critical as fighting has already begun to restart, threatening access to Idlib and stranding the aid amidst renewed violence. Khourari's contact recognizes how important HappyHelper's computers and IT equipment are to their core humanitarian mission. The lawyer transcribes Khourari's concerns into an email and searches his contacts for the right link.

The email eventually lands in the inbox of Francois Mittelstand of the CyberPeace Institute just before dawn breaks over his small studio apartment in Geneva two days later. Mittelstand had come to the young NGO from Deloitte, seeking to apply his decade spent working on IT security and incident response somewhere of humanitarian value. Mittelstand is the Head of Assistance for the CyberPeace Institute and has spent his first year in the young organization barnstorming around the world to build ties with humanitarian assistance and development organizations, in addition to regionally-based technology and security companies. These ties allow the Institute to partner with local and regional organizations who offer trainings, toolkits, and help engage in remediation efforts as part of the Institute's assistance work. Mittelstand has also been able to leverage connections with leading technology companies to offer free and low-cost versions of popular security and enterprise IT services to civil society organizations to help improve security practices and reduce vulnerability.

Mittelstand rolls over, still blurry from sleep, and scrolls his phone – looking for urgent mail. In the days since the WreckWeb attack began spreading rapidly from its initial victims in southern Europe, the Institute has been inundated with calls from organizations of all shapes and sizes seeking guidance and support across the globe. Mittelstand's phone is a portal to these cries for help and became a frequent target of the Frenchman's frustration as he worked to parse requests arriving faster than could be read. None had yet met the threshold of the Institute's guidelines for a response, some were universities with access to capable national CERTS, others were NGOs in large and developed countries who could be referred to full time assistance organizations. Members of the Institute's CyberVolunteer Network were working with a small Tibetan NGO that had been impacted, but Mittelstand had triaged the multitude of other requests to preserve the Institute's finite capacity to facilitate direct assistance to those who truly had nowhere else to turn.

Midway through his scroll, Khourari's request jumps out. The email depicts her call with the Turkish lawyer and a side note from the attorney about the importance of HappyHelper's work in the region as well as the short window of time the group has to deliver aid to Idlib. Not every cyberattack on a vulnerable group can receive direct assistance from the Institute. The Institute's charter focuses on attacks that cause significant and direct harm, those with broad effect that undermine people's trust in, and ability to gain value from, the technology ecosystem. Guiding the Institute's decision-making on when to act are the CyberVolunteer Network Guidelines – an internal policy developed by the Institute and its Advisory Board to help determine when to supply direct assistance and when to refer victims to other organizations better positioned to respond.

Racing through the email, Mittelstand matches phrases and reported details to the Guidelines, which have long since become a permanent fixture on the walls of his mind as well as his office. He realizes the event, and HappyHelpers' crisis, will more than meet the Institute's threshold for support and the machinery behind an Assistance response springs into action.

Recovery Coordination

Mittelstand makes the call that HappyHelpers' crisis, a result of the rampaging WreckWeb attack, warrants action by the Institute in accordance with its assistance Guidelines. Rendered in an email to the Institute's Chief Executive Officer, Mittlestand's judgement sets off a chain reaction. An alert email lands in the inbox of global partners as well as local volunteers in the Middle East/North Africa who work with the Institute. At the core of the CyberPeace Institute's assistance function is the CyberVolunteer Network, a regionally structured group composed of dozens of engineers, technicians, and information security professionals dotting the globe. These volunteers are largely full-time employees of technology and security companies, some of galactic scale enterprises like Amazon and Microsoft, but many others are members of small and medium size firms – Mittelstand's area of expertise. They work with organizations to deploy and maintain the Institute's toolkits and ensure organizations fully benefit from the enhanced security they offer.

The Network is regionally structured to be inclusive of volunteers who know the cultural environment and language of the groups they would be called to help. The Network has received a baseline training and participates in annual workshops with each other, both to enhance their own professional network, and to keep skills sharp – learning from recent assistance events and the experience of more senior volunteers. Upon successful vetting and selection by the Institute staff and a mini-advisory board of long-tenured volunteers from the Network, each new volunteer registers a profile with the Institute. Among other things, this profile helps define the volunteer's preferred geographic area of responsibility, their skills, and the status of their Institute NDA. Once selected members register a profile with the Network and sign the Institute's "Code of Conduct", agreeing to abide by the Institute's mission and values of delivering assistance impartially and independently. One of the unique, scaling, contributions of the Institute is that it negotiates a plug-and-play non-disclosure agreement between its volunteers, full time staff, and potential recipients of assistance who register beforehand. The document helps to speed assistance events and maintain a "trust bubble" over those volunteers and staff working to help a civilian organization recover without impeding the speed of the response.

Mittlestand's email to the Chief Executive Officer also notifies the Institute's event management staff to begin checking into the watch center. The Institute's watch center is a key part of the assistance strategy, providing a small pool of full-time staff to help coordinate the response of partner organizations and the volunteer network – providing critical event management and back office support to assistance activities. With the alert sent, Mittlestand replies to the Turkish attorney's email and lets Khourari know help is on the way.

In the next 48 hours, HappyHelpers are connected directly with three of the Institute's volunteers who will work full-time to help remediate the WreckWeb infection. One of those volunteers comes from a technology and security company based in Turkey with whom Mittelstand had previously established a partnership. As a result, he is able to recruit additional help from colleagues there who are willing and available to assist. Even without any full-time staff on the ground, the Institute's impact is significant as a project manager. Its volunteers wipe infected systems and install new operating systems and hardware. These efforts do not fully restore HappyHelpers visibility into getting aid to Idlib, but it's enough for Khourari to move ahead with the mission. The aid is delivered and saves lives. Meanwhile, the Institute continues to help get HappyHelpers back on its feet, Mittlestand introduces the HappyHelpers staff to a local IT security NGO for basic security training. Khourari tells a London newspaper, "Without the Cyberpeace Institute, people's lives were at a real risk; they made a difference here that cannot be measured only in pounds or euros. I trust their work and would recommend them to anyone who has nowhere else to turn."

Prevention

It's 6 months since that fateful morning. Mittelstand sips coffee from a small porcelain vessel above a windswept beach in Rabat. His work to build the Assistance function's network has only grown since WreckWeb. Not content to simply lurch from one crisis to the next, Mittlestand has helped his team and the responding volunteers package a set of lessons learned from the incident and their response to it. These are distributed to partner organizations registered with the Institute to help improve their capacity to respond to future events of this kind, and build new regional partnerships. These lessons learned include best practices for IT security, some of the automated configuration and recovery tools developed for HappyHelpers by the volunteers, and a link to one volunteer's dynamically updated priority list of the most recent major software patches. The registered organizations are able to access this and previous best practice packages through the Institute's secure online portal. Prevention efforts for the hundreds of organizations partnered with the Institute continue unabated, providing direct access to low cost security tools, and helping link vulnerable populations with dedicated capacity building organizations.

Prevention work is an investment in the future, Mittelstand knows, a way to reduce the horrors faced by groups navigating the consequences of the significant and direct harms of cyberattacks. Fatima's crisis was not the only one the Institute responded to during WreckWeb, nor was hers the last group to receive assistance from the CyberVolunteer Network in the months since. But by investing in prevention alongside response, there is a future for the Institute that helps build a more resilient and localized ecosystem of security-capable NGOs and not just an ever widening victim network to which it must respond.

Mittlestand knows the Institute has come together at a critical time, the next cyber event may be even more systemically devastating with physical effects far beyond those witnessed to date. His cup and its contents slowly cool as the Frenchman is lost in his thoughts, watching a string of ships bobbing slowly towards the Aboran Sea, wondering when the next attack will arrive.

CyberPeace Institute Function: **Accountability**

The Accountability function provides greater transparency into, and understanding of, an attack after it has already taken place and been mitigated in the hopes of supporting efforts to hold malicious actors to account. In the weeks and months following the WreckWeb attack, a decision is made by the Institute's Consortium to investigate the sophisticated attack, and the subsequent analysis provides the international system with an objective set of agreed upon facts to frame further discourse.

Consortium Activation

It doesn't take long for the computer threat assessment analyst to recognize a pattern in the network traffic scrolling across her screen. Leila is the newest member of Team Cymru, a prominent security company. Seeing the pattern, she gives up any hope for regular sleep, knowing she'll rely on caffeine and optimism in alternating doses to get her through the midnight shift in a dimly lit office space nestled in the suburbs of Eastleigh, UK. Leila's working through a dataset from France's National Cybersecurity Agency (ANSSI) related to the recent WreckWeb attacks. The stories about WreckWeb's fearsome impacts have receded from the news even as details of the viral pandemic have increasingly laid siege to her working hours. Working together with ANSSI, and other partners around the world, Leila's job is to understand the consequences of this global pandemic. That job brings her into close and regular contact with Aria, Cymru's permanent point of contact with the CyberPeace Institute.

In dissecting the ANSSI data, Leila discovers a series of infections of French utility companies that had gone largely unreported in the initial coverage.[15] She flags the pattern to Aria, who raises it with the Institute's Head of Accountability, Stefanija Dolenc. Dolenc is not technical by nature, her time before the Institute had been spent almost entirely within the humanitarian assistance community. An LSE grad, the cosmopolitan Dolenc had left university for a grueling series of internships with UNHCR and the International Crisis Group. Exhausted by the constant travel, the young Slovenian had landed with a humanitarian assistance NGO, HappyHelpers, and spent 5 years working as project lead and later country director in Pakistan. Dolenc was then handpicked as the Institute's first non-executive hire. Since then, she's shown a dogged commitment to highlighting the human cost of cyberattacks. She keeps finding new ways of understanding and detailing the human narratives in these attacks, the stories behind the numbers that have brought heightened media attention and scholarly rigor to cyberattacks that cause significant and direct harm.

[15] https://www.industrie-techno.com/article/notpetya-saint-gobain-tire-la-lecon-et-s-arme-d-intelligence-artificielle.53974

Dolenc runs a monthly call with the Institute's Consortium, a collection of private companies, civil society groups and academic organizations dedicated to better assessing and publicizing the consequences of large and harmful cyberattacks based on the collective intelligence and analysis capacities at their disposal. The group was largely self-selected, bringing together the individuals and organization with an interest, dedication, and capability to shed light on this often murky world. They operate under a set of strict rules, protecting the confidentiality and privacy of the data they deal with. On the call, the members discuss recent cyberattacks as candidates for analysis and review their ongoing work. Aria flags Leila's discovery and, together with requests from half a dozen other Consortium members, Dolenc puts WreckWeb on the Consortium's agenda to consider as a potential candidate for study.

It's less than a week later that Dolenc fields a call from the UK's National Cyber Security Centre (NCSC), asking if the Institute is looking at the WreckWeb event. For Dolenc the call does not come as much of a surprise. Since its inception, the Institute's accountability function has begun to fill a vacuum in the global discourse surrounding cybersecurity. Experts know that the Institute can provide detailed and well-grounded analysis of the consequences of significant cyberattacks. Its analyses have been cited in academic studies and media reporting. Although they may not say so, Dolenc knows governments around the world are among the most frequent consumers of the Institute's work. In some cases, they also contribute by suggesting directions or ideas for the Consortium to pursue. In this case, Dolenc's conversation with the NCSC proves to be one prescient. Over the next few weeks, she'll have similar conversations with government officials from France, Estonia and the United States. The agencies these officials work for want to know whether or not the Institute and its Consortium will be conducting an analysis of the attack that damaged many of their nation's organizations.

July's monthly call for the Consortium was long, but not contentious. Aria brings up the trends in WreckWeb's targeting that Leila had flagged. She suggests the attack is clearly worthy of further review. The group agrees by consensus, setting in motion a process to produce a compelling and thorough picture of WreckWeb's effects. Dolenc builds a study team from Institute staff and Consortium members, including Leila, whom Cymru has seconded to the Consortium for a several weeks long rotation as part of their partnership with the Institute. This frees her from her more corporate responsibilities like a number of other team members who hail from other large technology and security companies in the Consortium. Each secondment comes via an MOU signed by the employing firm and the Institute, detailing how much time from the employees' working hours will contribute to the study team, and the possibility of a full-term detail in the event of a crisis.

Dolenc also works to fuse data from the Institute's various corporate and non-profit members together with outside sources. Facilitating this cross-group sharing is a secure and carefully maintained collaborative analytical platform, the Institute's Clearinghouse.

Gathering Clearinghouse Inputs

Back at the contributing company's headquarters, Aria lets Leila know that the Institute is indeed moving forward with an analysis of WreckWeb and that she should share her data as appropriate via the Institute's Clearinghouse. Seconded corporate security analysists and university researchers have already begun to work through the Institute to study the WreckWeb event and Leila combs through the data her team has assembled from the event to share datasets that won't compromise ongoing investigations or violate her company's privacy policies.

The Clearinghouse is another of Dolenc's responsibilities and a key part of the Institute's value. Run on a hybrid cloud infrastructure and leveraging the latest technologies (including Artificial Intelligence), the Clearinghouse is a straightforward database and information sharing platform built on commercial cloud technologies. When a study team is stood up on a particular topic, the Clearinghouse houses all data related to the group's work from companies, non-profits, academics, and governments. When a study concludes, the data is archived and maintained for future work in accordance with the Institute's data retention policies. The Clearinghouse also captures insights from Assistance response activities to support proactive engagement with potential victim groups to help directly inform the Institute's advancement work.

Leila's dataset is a treasure trove of information on how the WreckWeb attack unfolded: samples of the program's code, records of a forensic investigation into the malware including sequences of instructions from its execution in a sandbox, and anonymized and aggregated records on the configuration of affected systems. Leila has also included information related to the impact of the attack on victims, including who was impacted and how long systems were typically compromised. The majority of the data provided by Leila's Threat Intelligence Team is sufficiently abstracted to fit into the Green and White categories of the US-CERT Traffic Light Protocol (TLP).[16] An analogous dialogue and cultivation of materials for the Clearinghouse takes place within other Consortium member organizations.

While Consortium members meet with their in-house teams, Dolenc and her staff at the Institute conduct outreach to third parties and consult public sources of data. Dolenc unleashes an awesome barrage of emails to key government ministries and points of contact at identified victim organizations to build impact profiles and lasso additional information about the attack and its victims into the analytic process. Constant Care Hospital Network, a US healthcare network responsible for multiple hospitals, supplies an incident summary about how their systems were compromised and anonymized information about the impact on patients.[17]

Dolenc focuses on driving as much good information to the study team as possible, leveraging the Institute's reputation as a neutral stakeholder and vast global network. She knows the Institute will not go so far as to attribute the attack to a named actor (the Institute's leadership and advisory board had decided early on to avoid such attribution claims to ensure its legitimacy among government actors). Thus, rather than engaging in the minutia of attribution debates for an incident such as this, and risk provoking conflicts between victim organizations and governments, Dolenc is able to drive the Institute towards analytic objectivity and crafting a compelling narrative while avoiding political morass.

[16] The US Computer Emergency Response Team (CERT) uses a "traffic light protocol" (TLP) with ratings of Red, Yellow, Green and White to describe the sensitivity of data in descending order, where Red is the most sensitive data and White is the least. The color codes indicate how widely information can and should be shared. https://www.us-cert.gov/tlp

[17] https://www.vox.com/2017/6/27/15881666/global-eu-cyber-attack-us-hackers-nsa-hospitals

Peer Review Analysis

More than seven weeks have passed since the study team was formed and began its work. Dolenc calls the monthly Consortium meeting to order, her voice clear over a digital phone line. “There’s a detailed outline and draft of the WreckWeb analysis report in the email I sent this morning” her words buzzing in the silence, “take time to organize your thoughts and responses but we should be ready to move to peer review”.

Dolenc’s request to the group is no small matter. Peer review, an academic process of area experts evaluating, commenting on, and even replicating each other’s work, is a lynchpin of productive research. The Institute leverages peer review both to socialize the Consortium’s analysis as well as seek expert criticism on complex technical judgements and broad impact assessments. Technical staff from respective Consortium members and several outside representatives selected by the Advisory Board work to determine where additional data is needed or a relied-on source may be suspect.

In the month following the call, technical experts from the Consortium's membership agree on how the ransomware attack was conducted, corrupting widely-used software and leveraging a repurposed exploit that had been developed by western military agencies to spread across networks, accessing credentials, encrypting data and locking-out users. They further sketch an outline for the scope of the attack, identifying where systems were impacted and for how long, including highlighting that nearly 75% of WreckWeb victims concentrated in three Eastern European countries. Reverse engineering from scholars at Dartmouth and University of California San Diego helps confirm some of the group's findings and identify new issues of technical significance.

A concluding report pulls together these technical analyses and provides as much transparency as possible about underlying methodologies and degrees of confidence in conclusions. Dolenc shares the report within the Institute while her team gets underway conducting an overall impact analysis.

Impact Analysis

As the Consortium members conduct their technical analysis, Dolenc coordinates her small team of policy wonks and social scientists to assess how victims lives were impacted by WreckWeb – mapping the social and community consequences of the attack. They explore the practical effects of the attack on day to day life, leveraging the Clearinghouse for data from both Consortium members as well as anonymized information from assistance response efforts. The team also conducts field research to capture a picture of the attack's impact on businesses and individuals in particularly impacted regions.

Dolenc and her team place calls to the Constant Care Hospital Network in the US, and interview consenting patients whose care was interrupted, delayed, or limited by WreckWeb. This research unveils the harrowing stories of multiple patients who had surgeries interrupted and even cancelled as a result of the attack.[18] The ensuing uncertainty and fear for these individuals and their families are indicative of the kind of emotional trauma an attack like WreckWeb can unleash and are captured by the Impact Analysis team's work.

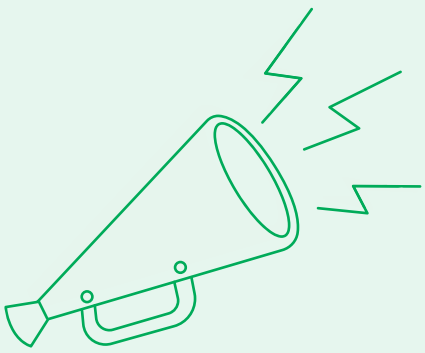
Beyond these personal impacts, Dolenc's victimology research includes further inquiries into organizations impacted by WreckWeb and uncovers businesses whose operations were interrupted, resulting in delayed services and billions of dollars in losses and other lost opportunity costs. Information provided by a global shipping company based in Europe details not only the immediate costs associated with the attack itself, but also lingering impacts in the form of delayed services and the financial impact of reputational damage running to hundreds of millions of dollars in losses.[19]

With these quantitative and qualitative analyses in hand, Dolenc is able to pull together into a holistic picture of the true consequences of WreckWeb. The impact analysis is one of Dolenc's tools to support the Institute's Advancement function, creating a human scale analysis of the damages from a systemic and harmful cyberattack. The impact analysis, alongside the Consortium's technical study in the peer review, represent the Institute's analytical work on WreckWeb and the logical conclusion of the Accountability function's mission. Dolenc shares the team's findings with the head of the Institute's Advancement work, who will be responsible for sharing them with the world.

[18] https://www.wtae.com/article/cybersecurity-incident-heritage-valley-health-system/10228015
[19] https://www.bleepingcomputer.com/news/security/fedex-says-some-damage-from-notpetya-ransomware-may-be-permanent/

CyberPeace Institute Function: **Advancement**

After WreckWeb, the Institute's Advancement function focuses on reinforcing international law and norms by calling out bad behavior and showing how attacks transgress rules, thereby strengthening the role the role of international law and norms in upholding responsible behavior in cyberspace.



Legal Review

Five months after the Consortium began its work on WreckWeb, the group delivers an interim report to Kal Sunghyon, the Institute's Head of Advancement. The child of North Korean refugees, Kal was a standout in school, receiving a scholarship to study computer science and international relations at Sciences Po. After a short stint as an electronics technician during his mandatory military service, Kal joined The Fletcher School's MALD program and encountered a burgeoning research group of lawyers and cybersecurity wonks. Their interest in cybersecurity norms would inspire Kal to focus his studies and attentions on this new policy space, where too few norms existed and where those that did were rarely enforced.

With the Consortium's technical and impact analysis of the WreckWeb attack in hand, Kal sets the Institute's advancement work in motion. The first step is a coordinated international legal review of the attack based on the Consortium's findings. Kal convenes a team of international legal scholars and technical experts to consider the conclusions of the Consortium's work as they relate to existing international legal regimes and rules constraining nation state behavior. The team Kal assembles is no standing body, but rather an unaffiliated collection of scholars and practitioners, who donate their time and expertise to help clarify thorny legal and normative analytic problems.

After several weeks spent debating the merits of various opinions and positions, the working group of legal experts comes to a consensus determination. The WreckWeb attack, as described by the Consortium, would appear to constitute a violation of Article 2(4) of the UN Charter – prohibiting the use of force in relations between States – if a government were determined to be responsible for the attack. In addition, the working group agrees that WreckWeb likely violated international cybersecurity norms as put forth in the 2015 U.N. Group of Governmental Experts' report on Developments in the Field of Information and Telecommunications in the Context of International Security by damaging critical infrastructure and impairing its use and operation by civilians. [20] The same norms which were subsequently codified as politically binding by some nations through the G7 and adopted by consensus by the UN General Assembly in resolution 70/237.[21]

20 http://undocs.org/A/70/174
21 http://www.g7italy.it/sites/default/files/documents/Declaration_on_cyberspace.pdf

Publications

With the technical, impact, and now legal analysis complete, Kal's team turns their attention towards the core function of the Institute's advancement work – making sure these findings are shared widely with a broad set of critical stakeholders, to be challenged, debated and reinforced as an authoritative account of the attack and how it should be understood in the international system. Kal knows that the months of work by the Institute's technical and legal experts are now relying on his team's ability to inject these findings into the global public consciousness.

Over several weeks, Kal and his team combine the Institute's various analyses to publish a summative report on the WreckWeb attack, detailing how it was conducted, who was impacted, and what the implications are for the perpetrators under international commitments; all without identifying or drawing conclusions about who was responsible for the attack.[22] The comprehensive report is published on the CyberPeace Institute's website and shared ahead of time with select journalists for exclusive reporting in influential markets. The full report emphasizes transparency in how the Institute's technical conclusions were reached and provides a well-annotated summary of the associated legal analysis.

However, while the full report provides a wealth of information to inform discussions in policy ministries and international forums, and is a feast for tech-savvy reporters, Kal knows the mission of the advancement work is to reach a wider audience and bring the Institute's conclusions into conversations around dinner tables across the globe. To this end, Kal works with graphic designers and communications experts to develop shorter, snappier versions of different portions of the report, as well as infographics and other multimedia, to showcase its findings.

The Institute leverages these resources to have its PR team engage various news outlets to further amplify the story of the attack and its consequences, and to keep the focus of the discussion on how victims were impacted and on how international obligations were violated in ways that should not be tolerated. From *Le Monde* to *The South China Morning Post*, to *Buzzfeed*, the findings of the CyberPeace Institute permeate a broad swath of publications, reaching a wide and diverse audience around the world.

[22] Publications may also track the extent to which attacks highlight any new trends or legal questions – such as the use of an exploit developed by the U.S. National Security Agency in the case of NotPetya.

External Engagements

Having widely published the conclusions of the CyberPeace Institute, Kal turns his attention towards advancing the issues of cybersecurity on the global stage by engaging key stakeholders in reviewing the Institute's findings on WreckWeb and considering their implications. This includes an initial gathering of scholars to discuss the CyberPeace Institute's analysis at its headquarters in Geneva.[23] In addition to affirming the conclusions of the Institute, this gathering explores how the case of WreckWeb reveals new gaps in international law and the international system. They recount disagreements about whether certain existing rules extend to cover WreckWeb, differences over what other applicable rules mean, alongside the reluctance of states to invoke them. The conclusions of these legal discussions have significant implications in an issue space with limited history or authoritative scholarship. Whether or not WreckWeb could be considered a use of force or even an armed attack, or if it falls below these thresholds will inform government decision making as they continue to iterate over appropriate and proportional responses.

Kal's team also continues to promote their findings by bringing together policymakers and other influential stakeholders alongside prominent multilateral and regional forums to share the conclusions of the Institute. Without advancing a particular agenda, the central question for these gatherings is as follows: if WreckWeb violates the expectations for responsible behavior in cyberspace, what can be done to strengthen these expectations to ensure that they are adhered to in the future to promote a safer and more secure cyberspace for civilians the world over?

Watching these dialogues progress between Cyber Ambassadors, UN country representatives, and others in positions of power, Kal is hopeful that the work of the Institute has helped set the stage for incremental progress, a slow shift in state and non-state behavior that leads to self-restraint and discouraging similar attacks from happening again and for leaders to take meaningful action when they do.

[23] Individuals and institutions may be brought together for such discussions alongside events like the expert workshop at the 2018 Munich Security Conference. https://cloudblogs.microsoft.com/microsoftsecure/2018/03/27/filling-the-gaps-in-international-law-is-essential-to-making-cyberspace-a-safer-place/

The Institute has illustrated in stark relief the harm caused by the WreckWeb attack and identified how far afield it sits from expected norms of behavior in cyberspace.

The stories of Fatima, Kal, Aria, Stefanija, Francois, and Leila, and the others described above, as well as the WreckWeb attack are fictious, but the victims of many other sophisticated cyberattacks are quite real. The CyberPeace Institute will breathe life into the these stories over the next 18 months as it stands up each of its three functions and begins to build the networks and depth of experience discussed above to enable its mission.