Cyber Collateral: WannaCry & the impact of cyberattacks on the mental health of critical infrastructure defenders

Tarah Wheeler & John, Lord Alderdice

On May 12th, 2017, North Korea unleashed a cyberattack of devastating size and impact on the United States. WannaCry was a ransomware attack that cost up to USD 4 billion, crippled law firms, rerouted ambulances, shut down one of the largest mobile communications operators in Europe, and (spilling outside the bounds of any intended cyber war zone) damaged the UK National Health Service with effects still felt today. Patients were turned away from hospitals, 13,500 outpatient appointments were cancelled including 139 screenings for cancer, and the information security professionals who responded that day remember it like the afternoon in 1963 that US President John F. Kennedy was shot or the morning of 9/11 when the Twin Towers came down. Overloaded technicians at British hospitals spent a week trying to keep emergency rooms open, doctors safe, and networks online. These frontline defenders kept the hospitals running, often by yanking laptops out of the hands of staff and replacing them with updated hardware as they ran through hospitals seeing a deadly red screen in office after office, patient room after patient room. Until a young British security researcher in rural Devonshire found a means to stop the attack, WannaCry infected computers faster than people could blink.

This paper represents the output of a US-UK Fulbright Cyber Security Award, to investigate Harm Reduction for Civilians during International Cyber Conflict. The project investigated the role of the IT responders to the attack, as the last line of defense for UK hospitals. Their stories were collected in a series of interviews conducted in early 2021. This paper provides an analysis and overview of how thin the defenses are between cyberwar and civilians, and a series of lessons learned and recommendations for improving the health and support structures for civilians who

have found themselves on the front lines. These attacks are continuing, and the lessons we've yet to learn from the previous attacks continue to visit our networks, homes, schools, hospitals, aerospace industry, and governments, growing even worse as the vulnerable targets remaining are the poorest-defended.

What happened

In the very early hours of the morning, UK and EU time on May 12th, 2017, North Korea launched a ransomware attack against the United States as a money-making scheme in the face of economic sanctions. Screens began turning red on Windows devices around the world, announcing that the data on those machines had been encrypted and would only be restored if the victim paid bitcoin to receive a decryption key. Initially, the attack was primarily felt in the EU and UK, as those parts of the world woke up, went to work, and turned on their computers, creating both the initial outbreak and the vector to spread infection.

WannaCry Ransomware Infection Heat Map

WannaCry was made possible by a vulnerability that existed in the Microsoft Windows operating system. Known as EternalBlue, this security flaw allowed attackers to implant and activate malware which could spread from computer to computer. On the day of the attack, while most security experts focused on patching this vulnerability within Windows, a young information security researcher on the west coast of England named Marcus Hutchins found a vulnerability inside the malware itself: he created a "sinkhole" which stopped the infection from spreading, preventing new machines becoming infected. In essence he deployed a 100% effective vaccine, but not a cure.

It was too late for many hospitals in the UK's National Health Service, which had already been infected. Hospitals began turning away patients, closing their doors, and canceling over 13,500 appointments.

At the time of the attack, detailed information from official sources on the nature of the attack and how to mitigate it was at least partially available, though much of it has disappeared due to link rot and updates. The UK's National Cyber Security Centre (NCSC), founded only a few months before in October 2016, had yet to develop a national incident response communication network. They had only been fully moved into their new office building for two weeks when on May 12th 2017, the UK's National Health Service tweeted a statement reassuring patients that their data did not appear to have been breached. The NCSC tweeted some guidance May 13th, 2017, but updated/removed pages even in news stories at the time make it difficult to establish and prove how much information was provided in the moment. One interviewee reported passing along information to a lower-level NCSC functionary who may have been able to act but did not acknowledge the information publicly. Guidance for enterprises appears to have been available, yet it is difficult to tell what was provided or when it was removed.[1]

[1] Ciaran Martin, then-CEO of the National Cyber Security Centre provided detailed remembrances of when and how information was delivered by NCSC to the public. Much of that information has been lost or written over due to UK practices regarding updating and deleting websites. The authors are grateful for the direction to resources no longer indexed by search engines or widely available; it certainly prevented errors of commission and omission while recounting dates and times of government communications.

When IT responders in NHS hospitals began getting reports in their hospitals, they turned to the Internet to find out what possible remediations existed. As a representative example:

> *It was Friday when we started hearing rumors of things happening in other hospitals. We didn't have a [network] security team. Our security efforts were nothing but the best efforts of employees keeping up with infosec on LinkedIn, Twitter, the usual word of mouth stuff.* [2]
>
> ~~ a front-line responder to WannaCry at a major UK hospital

Many respondents said they relied on potentially inaccurate or out-of-date information on Twitter to help them respond to the IT crisis, instead of any governmental guidelines – at least for the first week. Anecdotally, two Twitter accounts, belonging to Marcus Hutchins (@MalwareTechBlog) & Kevin Beaumont (@gossithedog), supplied much of the information accepted as useful and practicable by the IT responders in WannaCry.

To briefly summarize the technical issues at stake (more below), the challenge faced by responders was that a major vulnerability had been discovered in March, but not yet widely patched. Reliable patches were available but had been deprioritized in critical infrastructure in favor of ensuring systems were not taken offline for update, with the risk that patches might break interoperability. At the time of WannaCry, the cyber equivalent of 'the fog of war' descended on NHS hospitals, making it even more difficult to understand what was needed in the moment and if patching was a good idea.

> *We started to realize that we might be vulnerable. We had only just done our migration to Windows 7 and realized our stuff was ancient. We had a large amount of XP and S2003 and S2003R2 [systems vulnerable to WannaCry]. When we got the patch advisory from*

---

[2] While all interviews were conducted under conditions of anonymity to safeguard the identities of the respondents, some of whom are still employed in their fields in the UK, most gave permission to be quoted, and some gave permission to be named. All quotes here are reproduced with permission, with attribution according to the individual's preference.

> *MSFT to patch our stuff [in response to WannaCry], we went into overdrive. We got confirmation that Whittington or Imperial College had been hit, and we cut off all our links to the outside world, which included all other NHS agencies, patient care, everything. It was a complete assload of overtime and because of the age of the systems we're talking about, it was manually walking to them, manually installing updates/the patch, and it was a huge effort due to the amount of technical debt within the NHS.*
> ~~ a front-line responder to WannaCry at a major UK hospital

> *WannaCry was the moment the chickens came home to roost. Every bad management choice, every bit of underfunding, every lack of staff training and upskilling slammed home that weekend.*
> ~~ UK general responder

Incident responders in the UK reported near-total isolation and lack of information about what to do, and no public information that could help them advocate with their nontechnical executive leadership in order to explain the severity of the situation. In their own words:

> *No one was listening to us because it was a weekend. Our CTO [Chief Technical Officer] bought us pizza and left on Friday afternoon. We slept under our desks for 90 hours.*
> ~~ IT responder

> *The UK government wasn't in touch with any of the people doing the actual incident response.*
> ~~ Incident responder

> *Nothing from NHS Digital to help. We called, we waited, we emailed, we reached out again and again, and nothing from them. Not even a bulletin from the NCA or GCHQ.*
> ~~ Healthcare worker

> *We had a large number of workstations that we had to remove from users' possession as well. We had WIN10 [non-vulnerable] desktops in a cupboard, but these weren't deployed*

> *to users; the users all had XP [in that moment, believed to be vulnerable] desktops, and we started reimaging them all one by one.*
> ~~a front-line responder to WannaCry at a major UK hospital

> *It was a really stressful time, and it really highlighted the total lack of an infosec strategy. … One guy named [REDACTED, CTO role] was in charge of infosec but wasn't technical enough to understand what was happening and tended to simply follow directives. … As a department, we pulled an all-nighter for two nights, all the way through to Monday morning, and the best the Trust could do for us was buy us pizza. We went hands-on with every machine in the business. Thankfully we had no [WannaCry] infections, but it significantly impacted us because we had no plan in advance, no infosec strategy.*
> ~~UK general responder

> [describing the week of WannaCry, and the following week] *I didn't sleep for a week, and then I slept for a week.*
> ~~ UK general responder

Several of the interviewees responded that during the first week of the attack, they believed the UK government had only sent communications which reassured citizens that no data breach had occurred – basically, responding to the concerns of people that their healthcare data may have leaked rather than aiding the NHS in responding to the attack. The interviewees were likely referring to the NHS's 12 May 2017 statement mentioned previously. Incident responders were often undertrained and under-resourced, which left them vulnerable to misinformation campaigns such as that Marcus Hutchins created WannaCry, or that WannaCry was spread via email, or poor technical advice. An example of that last comes from UK security researcher and interviewee for this project, Daniel Card (@UK_Daniel_Card). He notes that at the time, there was a central directive from the NHS to unplug all connections to the Internet, leaving computers without access to the sinkhole which was stopping further infections. Even after responders, including Card, explained to the NHS that the only way to stop the infection's spread was to get back online to get

access to the kill switch, no one could or would authorize a change to the directive. That fundamental misunderstanding wasn't just in the UK. US cybersecurity expert Jake Williams (@MalwareJake) said the most "materially damaging" advice all responders were receiving was "to block the 'C2 domain' (in actuality, the kill switch) at network boundary devices."

Even experts with excellent professional skills lacked central support, which limited their ability to meet the crisis. Two interviewees reported being accused of incompetence when senior hospital administration did not understand their technical explanation of the situation.

One interviewee grew emotional when recounting that their hospital administration would not permit reconnecting to the internet, to take advantage of the Hutchins sinkhole. They carefully outlined how they had explained what had happened and asked us if they had done the right thing. The internal WannaCry infection persisted, and the hospital remained offline, rather than using the sinkhole to stop the infection. The interviewee wondered if they had failed to explain well what was happening to the computer network in a way that the nontechnical hospital administration would understand.

Technical account

Back at the beginning of this story, there were several unforced errors on the part of the US—not the UK—government. The EternalBlue exploit, which was at the heart of WannaCry, was originally developed by the US National Security Agency (NSA) possibly as early as 2012.

Instead of sharing the EternalBlue vulnerability with the global security community, the NSA shaped it into a secret weapon which escaped into the wild, along with several other NSA exploits, when the NSA toolkit was stolen and leaked by the Shadow Brokers. For the purposes of this discussion, WannaCry is comprised of EternalBlue plus a worm: the vulnerability was paired with replicating code that could spread unchecked. While WannaCry has been attributed to the North Korean Lazarus Group, these same stolen NSA tools (including EternalBlue) formed the core of the June 2017 NotPetya attack, perpetrated by the Russian military. Arguably even more financially and globally devastating than WannaCry, NotPetya is the second generally-accepted

act of cyberwar attributed to a country. The first was Stuxnet, an extremely sophisticated computer attack by the US on Iranian nuclear centrifuges.

The Lazarus Group, behind major hacks such as the 2014 Sony hack, still exists and appears to be motivated by causing chaos and profit, though WannaCry cost more than it gained them.

Timeline

Prior to August 2016

Some time before August 2016, a computer crime group called the Shadow Brokers hacked into and stole a substantial package of Microsoft exploits (including EternalBlue) from the Equation Group, which is widely understood to be part of the US National Security Agency.

March 2017 - Microsoft patches a major flaw, quietly.

On March 14th, 2017, Microsoft added a major patch to Windows with no public statements or press release beyond the standard blog post for all CVEs (Common Enumeration of Vulnerabilities - the numbering standard for publicly disclosed vulnerabilities that includes information on mitigation).

This patch addressed a critical flaw that should have had wide attention: the ability to execute code directly in the operating system, remotely. If every eligible Windows system had automatically immediately installed this update, WannaCry (and NotPetya) would have had vastly reduced impacts, and perhaps never would have been released at all.

April 2017 - Shadow Brokers leak

Several of these exploits, including EternalBlue, were leaked by the Shadow Brokers in April 2017. Notably, the patch from Microsoft was a month before the Shadow Brokers leak. It is believed that the NSA had found the original vulnerability more than five years earlier, but only chose to alert Microsoft after it suspected EternalBlue had been stolen – triggering Microsoft to delay its usual February "Patch Tuesday" until March. The lack of fanfare around the March Microsoft patch might have indicated that the NSA and/or Microsoft preferred not to draw attention to the flaw: regardless of the reason the patch was released quietly, Microsoft was aware that exploits like this were possible long before the public knew. This is not to say that Microsoft intended to hide the severity of the vulnerability, only that there are many reasons – some public-spirited and appropriate – that they could have chosen to patch quietly rather than call attention to the severity of the situation.

Technical importance

Most vulnerabilities pose limited risk in isolation: linking a chain of vulnerabilities together into an exploit that produces the desired effect requires effort and specialist knowledge. Imagine a very complex anti-aircraft missile. Giving the parts to someone who hasn't ever built one probably won't do too much harm, at least right away, and a problem with any one component renders the weapon inoperable.

EternalBlue, which was the heart of WannaCry, was not simply a theoretical vulnerability: the exploit had been highly developed by the NSA. It was more like handing over a shoulder-mounted Stinger surface-to-air missile with two labels on it: 'point this end at bad guy' and 'push this button to fire'.

Windows 7							
Windows 7 for 32-bit Systems Service Pack 1 (4012212) Security Only[1]	**Critical** Remote Code Execution	**Critical** Remote Code Execution	**Critical** Remote Code Execution	**Critical** Remote Code Execution	**Important** Information Disclosure	**Critical** Remote Code Execution	None
Windows 7 for 32-bit Systems Service Pack 1 (4012215) Monthly Rollup[1]	**Critical** Remote Code Execution	**Critical** Remote Code Execution	**Critical** Remote Code Execution	**Critical** Remote Code Execution	**Important** Information Disclosure	**Critical** Remote Code Execution	3212646
Windows 7 for x64-based Systems Service Pack 1 (4012212) Security Only[1]	**Critical** Remote Code Execution	**Critical** Remote Code Execution	**Critical** Remote Code Execution	**Critical** Remote Code Execution	**Important** Information Disclosure	**Critical** Remote Code Execution	None
Windows 7 for x64-based Systems Service Pack 1 (4012215) Monthly Rollup[1]	**Critical** Remote Code Execution	**Critical** Remote Code Execution	**Critical** Remote Code Execution	**Critical** Remote Code Execution	**Important** Information Disclosure	**Critical** Remote Code Execution	3212646

Figure 1: Criticality assessment for EternalBlue

Process failures and lingering questions

Of the companies that were vulnerable to WannaCry in 2017, 26% of them were *still* vulnerable in 2021. That means more than a quarter of the companies who learned that their computers were at risk of infection from WannaCry still have not updated their vulnerable systems.

These systems administrators deliberately did not update—and are still not updating—their computers. In many cases, this is because the machines *cannot* be updated: in NHS environments, updating Windows may break compatibility with proprietary software on medical equipment such as CT scanners, or accredited dataflows – and this problem is common across many industries with computer-enabled Industrial Systems infrastructure that lasts longer than the typical software maintenance lifetime. IT security teams take steps to isolate and protect those machines in other ways – but they are obliged to work around software they know is vulnerable. As an example, more than half of all IoT-enabled medical infusion pumps are currently vulnerable to critical exploits, but updating those devices is often difficult, vendor-prohibited, or not possible to do remotely.

There is a further process failure, regarding how individuals are informed of serious cyberattacks and the impact on them: GDPR has clear provisions for dealing with data breaches but is silent on other forms of interference with data. In one interview, a patient at the time related that the data from their previous cancer scans, including all the imagery, had disappeared, and the customer service advocate on the phone said that it was due to WannaCry. Since the hospital had not experienced a *loss of that data due to a third-party breach*, but had in fact had its data functionally deleted, there was no requirement and certainly no incentive to inform patients that previous years of scan and diagnostic data had been lost in the attack.

Many people in the UK have missing medical data about which they have never been informed: their data was lost or destroyed as part of WannaCry, but because no breach occurred, there is no legal responsibility (or clear best-practice mechanism) to inform them.

Our approach to medicine and health tends to be individually orientated and since there is no way to code on a death certificate that it happened from a cyberattack - just as subsequent development of cancer some time after the 9/11 attacks or adverse health outcomes from COVID that are not related to individual infection are not, and cannot, be coded on a death certificate, despite them being connected. The only obvious way of making assessment of impact is through the measurement of excess deaths during a particular period or geographical region and the connection/causality cannot be definitively proven in the usual way.

The absence of a universally agreed-upon mechanism for national accounting of the impact of health data loss/breach due to cyberattack is not just an issue for health authorities. Militaries and governments have also no clarity about how to calculate the loss and harms of this kind of missing data as part of the impacts of an act of war.

We must also train executives in how to receive and implement technical advice from their experts rather than undermining the infosec staff's confidence and overriding their efforts. Daniel Card notes that during the height of NHS incident response, all NHS responders were instructed to disconnect from the Internet, rendering the kill switch unavailable even though "it was apparent that disconnecting from the internet in this scenario was not a good move and it hindered response

and increased negative impact." Responders suffered then, and still suffer, from difficulty communicating technical concepts simply enough for executives to believe them, and for those executives to have a pathway to respond positively to this information.

The current situation in the UK and USA

The NHS is attempting to learn the lessons of the past by improving their security stance NHS trust by trust. Across the border, that did not save the Irish hospitals experiencing ransomware attacks in June of 2021.

The recent release of the 2022 UK national budget shows improved spending in IT and information security. But there's still a gap between the kind of training, equipment, and staff outlay that would be needed to address the next cyberattack.

By contrast, in the US, small and medium medical businesses are told, in a dystopically capitalistic turn of phrase used sarcastically by one interviewee, that they have their 'choice of providers' to assist with cyberattacks. Private contractors are performing as an *ad hoc* civilian defense force, but conceptualised as an outsourceable commodity, like food service or landscaping. There is no US "civilian cyber" equivalent of the Joint Interagency Coordination Group – or even HIPAA – to coordinate, guide or evaluate this activity across hospitals (or other industries).

Information sharing and community response

Interestingly, one interviewee said that if the NHS had begun treating cyberattacks as predictable events with seasonality and varying impacts – like flu – they would likely have been more prepared.

In terms of a top-down and community response, the immune system of the global beneficial information security community was lacking in May 2017. A coherent and cohesive strategy of communications and response could have aided in this crisis. This is one lesson learned: the UK

NCSC emerged from WannaCry (and NotPetya one month later) with a clear mission, and was catalysed to develop a highly informative website and other initiatives like the Cyber Information-Sharing Partnership (CISP). .

There was a gap between the ways that incident responders get information in information security, and the ways formal information was being produced and distributed at the time. Despite the diligence and hard work of the people at the NCSC, in the NHS, and in IT all over the UK, there were major 'process gaps' that resulted in failures to connect them all together at times of dire need. The NCSC twitter account clearly mentioned WannaCry that week, but there are serious historic and archiving issues with retrieving how much information was provided and when. By May 19th, 2017, they had released guidance on how to patch and what to do in the event of an infection.[3] By contrast, the United States has yet to release any overarching government guidance on WannaCry or any after action report explaining how the vulnerability impacted US critical infrastructure. While CISA releases guidance every so often on specific threats, general instructions often come from NIST, which moves relatively slowly compared to the nature of cyber threats.

Our interviewees showed a strong preference for fast-moving updates (especially Twitter). Anecdotally, it is still the case that industry professionals keep up with cybersecurity news via social media.

[3] Links to other resources on this page are broken, including the link to the patch page at Microsoft. This link https://technet.microsoft.com/en-us/library/security/ms17-010.aspx does not exist any longer, though any information security professional knows that the vulnerability number reference 17-010 refers to EternalBlue. Here is a link to the ongoing patch page: https://docs.microsoft.com/en-us/security-updates/securitybulletins/2017/ms17-010

Bypassing the military

It is not only the NHS that is in the process of mopping up half a decade after an international disaster. While it is true the NHS was a soft target due to lack of focus on cyber security, the health service should not have been under fire in the first place. In any other field of conflict, under international law, hospitals are required only to be clearly marked – not situated in an underground bunker.

In 2022, critical infrastructure components still have ancient vulnerabilities that have been left unpatched to ensure uptime. There is a deep emotional and professional exhaustion amongst IT responders. They feel alone in front of the civilians they are protecting, as they respond to acts of war that have bypassed the military.

Relying on lone independent security researchers to hopefully find solutions to messy cyberattacks damaging civilians is surely not the right way to prepare steadily for a future of increasing ransomware attacks. Since 2017, attacks have increasingly targeted civilian infrastructure, ignoring Rome Statute 8 of the International Criminal Court which prohibits attacks targeted towards hospitals and medical installations. In 2020, healthcare was the seventh most targeted sector in the world, with cyberattacks doubling over the course of the year (more recent statistics have not yet been tabulated). The massive cyberattacks against hospitals in the United States in October 2020 intended to disrupt and damage US critical infrastructure in the days leading up to the 2020 presidential election show that not only can attacks spill over into hospitals, but they will sometimes be targeted deliberately.

We must guard against two extreme positions: the idea that major cyberwarfare has not yet happened, as well as the idea that these attacks are inevitable and so low-level that they do not matter in terms of geopolitics.

Models for civilians coping with irregular warfare

The role and resourcing of IT responders in cyber conflict can be framed in a wider conversation about civilians dragged into low-impact, high frequency warfare and the long-lasting impacts on health, safety, and community.

What sorts of lessons have we learnt in other situations about civilians coping with irregular warfare?

1) Individuals need to make some sense of what is happening to them when in a low-level, high frequency conflict? Most people need to feel part of a larger story in the conflict. Unfortunately this usually involves some demonizing of the 'enemy'. We have noticed a rising anti-Russian sentiment among infosec professionals, with more racist memes, othering, and hostility. It may be difficult for an individual do other than become part of this culture of increased hostility unless they have some alternative internal structures of a religious/artistic/social/educational nature, but then they will likely come into conflict with their own surrounding group. For this reason we need to look at the larger communal relationships.

2) At the level of communities, companies, and countries, are there any lessons that can be learned from successful peace processes such as the one in Ireland which emerged from 'the Troubles' there and culminated in the 1998 Good Friday Agreement? The first lesson is that both sides need to have reached a 'hurting stalemate'. If either side thinks they can win out by violence there is little basis for negotiation. When this context finally emerges, one way into constructive discussions can be to address common human needs like working on shared economic development, with inward investment to rebuild after the conflict, improving infrastructure, health care and personal security.

3) While there is no evidence that the various geo-political opponents have yet reached a 'hurting stalemate' – far from it - similar methods can help sustain internal community relationships and well-being. Given the continuing attacks in cyberspace might it be important for NCSC and/or CISA to mandate and fund technical education and mental health care for critical infrastructure SOC (security operations center) analysts and DFIR (digital forensics and incident response)

specialists? These people are watching out for and investigating the aftermath of cyberattacks and we need to ensure their well-being. Looking after them may not only keep critical infrastructure such as water or nuclear power safer, but also make our defenders feel appreciated and supported with outcomes improved as a positive externality of focusing on humanity and community support. Eventually, if there was some kind of cessation of hostilities, we would also be prepared with educational and mental health support strategies which could facilitate humanitarian engagement with adversaries, just as with the Marshall Plan did after the Second World War. In cyberwar the destruction may be different from that seen in carpet-bombing, and the reconstruction and repair may be as much of relationships and well-being as of hardware.

Recommendations

Recommendations for the UK

The UK responded to and created a solution for WannaCry before most IT security professionals in the US even woke up on Friday morning, but has only partially learned from that crisis. The US is insufficiently prepared even for what it would have faced in 2017, much less 2022. Based on the results of these interviews, and other conversations within the IT security community, it seems likely that without a focused policy response, the first responders will be exhausted, burnt out, and demoralised when the next crisis comes.

In our interviews, IT responders described a climate both before and after WannaCry where it was difficult to make a case to allocate funds to information technology and security, instead of critical care. Even after WannaCry, it is difficult to convince NHS Trusts that the lack of patched and updated technology might mean critical care must be denied to everyone. Individual trust support is being provided by NHS Digital in a program that is no longer funded centrally. Currently, there does not appear to be a line item allocation of budget for cyber security specifically dedicated to the NHS in the 2021 Autumn UK budget review, and priorities post-COVID are in flux.

Recommendations for the US

The United States has yet to implement the fixes for the lessons learned by the United Kingdom. Other than one reporting portal and two-yearly contract appointments for two individuals at the Cybersecurity & Infrastructure Security Agency (CISA), the US has no functional way to help or mitigate healthcare-targeted ransomware or nation-state cyberattacks other than referring hospitals and GP practices to whatever free market solution seems best. Current guidelines direct companies to purchase managed security services from any provider available, and those services vary widely in their ability to assist competently. In the United States, there is still little guidance on what to do in the event of a major cyberattack, and mandatory reporting of cyber incidents was only announced in March 2022.

The US needs to have a more official channel to dispense and disperse information about ongoing attacks, and it needs to be the Twitter account or blog of record – in other words, something quickly updatable, accessible to and trusted by incident responders. Both US and UK responders repeated that they were getting their information on Twitter from information security influencers like GossiTheDog and MalwareTech. They were indeed good sources of information, but national security resources should be leading the narrative. The UK learned this lesson, and now the NCSC blog is incredibly helpful with its case studies, up-to-date bulletins, and most importantly: rapid updating of recommendations when needed. One of the primary reasons the US State Department's Fulbright program exists is so that senior scholars can exchange ideas and bring back new practices and policies helpful to their home countries. In the opinion of the American author of this paper, the US CISA blog, which functions more as a press release outlet, could learn some lessons from how NCSC does it.

At a bare minimum, the US could address the uncertainty around reporting flagged in our interviews: currently there is no obvious channel for healthcare cyber security reporting. We understand from CISA that it is meant to fall under "critical infrastructure" but anecdotally many IT professionals would instinctively report events under "private industry" since the US health system is privatised. We recommend CISA add a "healthcare" option to the dropdown in the critical infrastructure reporting form found here: https://us-cert.cisa.gov/forms/report.

Finally: US health facilities are potentially legally liable, if admitting to not having trained personnel or current equipment – whereas the NHS does not have this same risk. Let us consider expanding the no-fault reporting abilities of CISA to the mandatory critical infrastructure reporting requirement recently signed into law by the Biden administration.

Overall Recommendations

In both the US and UK, the healthcare IT ecosystem is set to remain in the care of local IT administrators. It is not possible to command and control the civilian IT security process without moving to a centralized command economy. Therefore, we must psychologically arm and ethically train IT professionals, so they have avenues to report events, seek advice, and communicate best practice in ordinary and emergency situations.

Incident response from WannaCry continues even now. Outdated operating systems on critical infrastructure are still vulnerable to WannaCry and would even now be infected if Marcus Hutchins was not maintaining the sinkhole domain. Resources are not being allocated to update these critical systems upon which healthcare, water, power, and other infrastructure depends. That drains the people who have been working on it for years, emotionally and professionally. Support for civilian defenders of critical infrastructure, including for mental health and burnout, in the United States and the United Kingdom does not yet exist in any meaningful way.

Conclusions

After a three-month journey of interviews and research, our conclusion is that the NHS is still recovering from a monumental cyber war crime, and it was only the actions of a few heroes in 2017 that saved hundreds, perhaps even thousands of lives. Clapping for the NHS during the COVID-19 pandemic aside, the NHS sysadmins all along have needed budget and belief and backing, and they are only now beginning to receive it. In the US, individual health care IT workers and infosec incident responders are still largely neglected.

The 2017 WannaCry attack was a devastating nation-state-level act of war against a civilian population. Our interviews with the IT defenders and responders in the UK's National Health Service show that these IT responders were and are a front-line, a core component of national security. Furthermore:

1) these attacks are bypassing traditional military installations and being directed at soft civilian targets
2) there is a need for international collaboration and community response, recognising that cyber-attacks can constitute low-impact, high-frequency warfare, and
3) globally, IT responders are not being supported and recognized for their roles in defending civilians against state-sponsored cyberattacks.
4) even as we completed the write-up of this paper NHS 111 (the system used for referring patients for care, dispatching ambulances, out-of-hours bookings and emergency prescriptions) experienced a software outage caused by a cyber-attack.

Recognition comes with a realisation that this is a real and present danger, and the implementation (not just the planning) of policies, solutions, budgets, industry development, and training.

Providing such 'recognition' is an urgent necessity.

APPENDICES

Acknowledgements

The authors wish to acknowledge Katherine Fletcher for her personal and professional heroics in getting this project hosted at the University of Oxford and completed during an extraordinarily difficult lockdown period in the midst of the COVID-19 pandemic. Without her, this project would not have been accomplished.

We would like to thank (while retaining all responsibility for any inadvertent errors or omissions) the extraordinary people both named and anonymous who provided background, interviews, technical assistance, support, and connections.

Thank you so much to Kat Duffy for editing and support, NHS architect Jagdip Grewal for connections and time and a pointer to the internal structure of the NHS Digital service, Simon Newman at Police-CPI for statistics on cyber-crime in the UK, Mary Branscombe & Simon Bisson for generosity of time and spirit as well as the largest Rolodex in all Albion, Henrik Kiertzner for the overarching picture of UK healthcare cybersecurity and the brilliant question: "How does a GP in the UK know when they're ***not*** experiencing a cyberattack?", Pete Coleman at Great Ormond Street Hospital for brilliant conversation and an explanation of how the NHS handles research allocation in crisis, Rob Johnson at the Changing Character of War Centre for encouragement and pointers to the right people to speak to as well as confirmation that mental health is part of cyberwarfare victimhood—an excellent reminder that not all harms in cyberwar are immediately visible, Josh Corman, CISA head of response for cyber and COVID-19 for the shove in the correct direction, Artis International head Rich Davis for clarity and a lovely conversation, Deviant Ollam, Kim Zetter, Janet Hutchins, Alexsis De Raadt-St. James, Tom Chadwick, David Hobbs, Ian Wallace, Allan Friedman, Jon Callas, Greg Conti, Anne-Marie Slaughter, Daniel Card, Ciaran Martin, Zack Whittaker, Marcia Hofmann, Janis Machala, Scott Larson, Jamie Collier, L. Jean Camp, Ross Schulman, CJ Guthrie, Laura DeNardis, Lauren Zabierek, Gresham College, the University of Oxford, Beau Woods, Siân John, Laura Louthan, Stacey Wright, Danny Palmer, Jake Williams, @admford,

those who cannot be named here,

all the incredible people at the UK National Health Service and across the United Kingdom and United States, especially our infosec family,

And finally, to Marcus "MalwareTech" Hutchins, for saving the world, a lot.

Origins of this study and COVID-related methodological issues

One author here, Tarah Wheeler, proposed a series of interviews of WannaCry responders in mid-2019 to the US/UK Fulbright Commission, and in collaboration with John, Lord Alderdice at Harris Manchester College, Oxford, and institutional sponsor Katherine Fletcher at the University of Oxford's Department of Computer Science, was awarded a Cyber Security Fulbright to provide social science data on the ongoing effects of low-impact, high frequency warfare on civilians. The other author, Lord Alderdice, one of the original drafters of the Good Friday Agreement and a practicing psychiatrist and director of the Centre for the Resolution of Intractable Conflict in Oxford provided a historical and psychological context in which this study could be placed by using the lessons learned from the Irish Peace Process about dealing with low impact, high frequency warfare on civilians in Northern Ireland.

In interviews conducted between January and April of 2021 with personnel from NHS Digital, patients who experienced the impacts of WannaCry at the time, NCSC personnel both former and current, US Critical Infrastructure & Security Agency personnel who were their counterparts in 2017, independent security researchers in the UK, US, and Europe, former Metropolitan Police personnel, doctors, and—most importantly—multiple 2017 WannaCry incident responders, we asked multiple key questions about the nature of the incident and how the response worked or didn't.

The constraints of COVID-19 on interviews were profound and some intended interviews were cut short or could not be conducted, due to this project beginning Jan 3 and extending to April 16th, 2021. The UK COVID lockdown unexpectedly began Jan 4th and ended April 11th, which meant all interviews were conducted via video to wherever the interviewees were located in the US and UK.

The constraints, however, actually gave rise to an extremely interesting additional methodological discovery. At least three of the interviewees gave a rough estimate that on May 12th, 2017, there were less than fifty people in the UK who were qualified to and capable of responding on a technical leadership level to the WannaCry ransomware attack. Unable to visit any NHS hospitals

or installations, we used snowballing interview techniques to find and video interview five people who directly responded to WannaCry in the UK, and approximately thirty other people associated with the NHS, the UK government response, journalists at the time, US equivalents to NHS responders, and academics in cybersecurity. Though five people is not enough for statistical analysis, by anecdotal evidence we tracked down and spoke to a tenth of the people in the United Kingdom who could shed light on this topic.

While this project was deeply limited by COVID and the fear of losing jobs made some participants who had been willing to speak in person not comfortable with speaking via video, the conditions actually made it ideal for a meta-experience of being locked away from resources and trying to find out where the gaps between practice and theory lay at the time.

While there cannot be a meaningful statistical analysis of 5 people, there are some frequently-repeated themes in the interviews which in the authors' experiences and other research are extremely relevant to civilians who find themselves in conflict anywhere.

Instead of using traditional qualitative and statistical methods to present our conclusions, we have asked for expert review and validation from people in a position of leadership both during WannaCry and in other parts of government, civil society, academia, and industry to strongly encourage a review of the mental health and work support resources available to the civilian incident responders in cases of nation-state cyberattacks.