e-Health as a target in Cyberwar: Expecting the worst in the COVID-19 Pandemic

The use of e-Health creates vast potential to transform health care systems and advance clinical outcomes and service delivery. In particular, with the global spread of SARS-CoV-2 virus that causes COVID-19, the influence of health ICT is expected to be significant, for example, in minimising the risk of spread through close contact using Telehealth [1], and containing its spread through the use of contact tracing apps [2]. However, McGraw [3] argues that such ICT integrated systems not only harbour a lot of vulnerabilities that increase cyber threats, but our growing dependence on them is a key factor that makes cyberwar against such systems unavoidable. While this might seem far-fetched, e-Health can potentially be a target in cyberwar. At a strategic level, a cyber-attack on e-Health could compromise the integrity of data and systems, privacy of patients (through exposure of sensitive personal data – which might include key personnel within the government or the military), or the disruption of critical facilities. From this, one fundamental question arises: ***What would be the impact of weaponizing e-Health in the context of cyberwar?*** To explore this, the article will examine the concept of e-Health as a critical infrastructure within the society and its potential use and abuse in the context of cyberwar.

Traditionally, the delivery of healthcare services depended on offline files and paper-based records, which led to discrepancies and inefficiencies [4](p.16). For example, previous contact tracing approaches were paper-based [5] which led to finite data collection, storage and access, poor data quality and privacy concerns. This was later changed and improved through the implementation of e-Health. According to Ossebaard and Van Gemert-Pijnen [6], e-Health refers to the use of information and communication technologies to support health, well-being and the healthcare system. These technologies span from those offering storage of Electronic Health Records (EHRs), medical devices, mHealth applications, and telemedicine [7], to the reinforcement of secondary processes of care, such as, booking of appointments and case management [6]. As a result, e-health supports consumers with improved access and control over their health by emphasising self-management, involvement, and transparency [8], while at the same time providing healthcare professional with an opportunity to make clinical decisions and improve consumers' welfare [4, 9]. As such, e-Health is regarded as a critical infrastructure as it is vital for the functioning of the society in terms of healthcare services delivery and public health. Its disruption can destabilise a society and at the same time put the national security at risk as it is often, among other critical infrastructures, considered as a preferred military target [10].

Evidently, there has been major improvement in the healthcare system attributed to disruptive technologies and in the dawn of COVID-19, people will rely more on e-Health in a number of ways. For example, [11] and [12] explain the importance of e-Health solutions such as Telemedicine in sustaining the capacity to provide health services not only to those stricken with COVID-19 but also to other patients suffering different conditions while still maintaining 'medical distance'. Further, [11] claims that the use of e-Health solutions during this global pandemic will help healthcare consumers obtain significant health information which could help them achieve better mental health and quality of life. In addition to this, public health officials are utilising the ubiquitous nature of smartphones to trace and identify individuals who have come in contact with an infected person by using contact tracing apps for COVID-19 [13]. With all these benefits and more, the digitisation of healthcare never lucks a downside that puts it on a tough and revealing test. Coventry and Branley [7] state that the cybersecurity infrastructure of the healthcare is wanting. This is attributed by an increase in interconnectivity, which exposes the sector to not only common but also to new vulnerabilities that put the security of health data and mobile medical devices at risk [14]. Further, taken in isolation, disruptive technologies in healthcare tend to introduce unanticipated vulnerabilities that create more cyber threats. According to Liff [15], attacks that use these vulnerabilities in computer networks can be exploited in cyberwar. These threats present opportunities for attackers to gain access to the network with the intention and different motives of compromising e-Health.

In their work, Sevis and Seker [16] state that attackers compromise critical systems with the intention of pilfering, damaging or taking control of critical information. In the context of e-Health, the health data contains extensive information, and unlike financial data, resetting certain identifiers, for example, name and address is impossible [17], which makes it a potential target for attackers at different levels. Further, while the contact tracing apps and other contact tracing methods claim to protect the identity of possibly infected people and the people they encounter (which is arguable), a person's health data can reveal whether they have had or have the virus.

Therefore, exploitation of health data is conducted for several motives and with different outcomes. With the health data containing extensive source of valuable information, Martin et al. [17] indicates that financial gain is the key motive for compromising healthcare systems. Further, taken in isolation, contact tracing methods have also been highlighted by [18] as channels that provide opportunities for bad actors to commit both fraud and abuse. Hence, a cyber-attack launched by non-state sponsored and opportunistic adversaries would have the following consequences and impact as listed in Table 1:

Consequences	Impact
Active surveillance – collecting PII and COVID-19 data	- Cybercrime - Random people targeted for medical identity theft and medical fraud insurance [7]. - Identity theft from COVID-19 related data. For example, COVID-19 patients' personal data released to the public through texts like in the case of South Korea could be use by attackers to commit identity theft [18]
Personal attacks derived from PHI and COVID-19 data	- Cyberbullying – intimidating individuals with harm [19] especially with the stigma surrounding COVID-19. - Stalking of an individual based on supplied contact tracing data [20]. - Blackmailing – which might result to psychological and physiological effects [19] or even financial harm. - Harms to dignity or reputation as explained by [18] when data released by South Korean government sparked unpleasant rumours about certain individuals. - Location data derived from tracked mobile phones can be used to reveal an individual's identity, frequent location and health information based on where one visits for treatment and hospital care [21]
Disruption of medical services [14]	- Interrupted online appointment resulting from compromised telehealth systems. - Generation of spoof transmission to create logs of false contact events. This was identified as a risk on one of the contact tracing apps [22] - Interrupted access to laboratory tests, for instance in the case of LifeLabs [23]. This can be a problem when healthcare professionals want to access COVID-19 related test results.

Table 1: Consequences of lower-skilled cyberattack against e-health.

However, in an age where global awareness of cyberwarfare has increased abruptly [24] cyber-attacks can not only be driven by political or financial gain, but by the ability to take lives [7]. State-sponsored attackers normally perpetrate these attacks. According to the Journal of Law and Cyberwarfare [25] pg.6, "state-sponsored attackers go after high value information that will give their countries a competitive and military advantage such as, intellectual property, classified military information, schematic drawing, etc." This is indicative that they are driven more by strategic rather than financial gain.

As such, health data exploited in this case can have severe consequences and impact listed in Table 2: In addition to these consequences, data collated by public health officials and stored in central databases or websites can be maliciously used in the context of cyberwar. For example, South Korea has maintained a public database of known COVID-19 patients, including their personal data, such as name, occupation, and travel routes [26]. While this might seem like a great move to reduce the spread of COVID-19, such information can be used to influence or manipulate the epistemology of the society, for example in the case of information warfare campaign at a strategic level [27].

Consequences	Impact
Active Reconnaissance – collecting PII and COVID-19 related data from health data and central databases for enemy intelligence.	- Key people targeted (either government or military), for example, The Trident Juncture 18 [28]. - Building a database of targets for further exploitation of PHI and personal data derived from COVID-19 central databases and websites. - Attempts to steal COVID-19 research data and intellectual property [29]. - Location trails uploaded to COVID-19 databases can be used to locate sensitive sites such as military bases and secure research laboratories [18, 30]. This could be used as a powerful planning tool for enemy intelligence - Location data derived from certain tracking apps and mobile phones can be used to track certain individuals and deanonymize them [31].
Personal attacks derived from PHI and centralised COVID-19 databases.	- Deanonymisaton of individual from location data derived from tracked phones and apps can be used to perpetrate revenge thus threatening the safety of the said person [30] - Prescriptions and personal medical records can be altered [19] with nefarious intentions of putting the patients' safety at risk. - Disclosure of medical files. For example, the case medical files stolen from the World Anti-Doping Agency [32]. - Medical devices, for example insulin pumps or cardiac pacemakers, can be targeted and their data manipulated [33], which could be fatal or lead to physiological effects. - Black mail and extortion resulting from the COVID-19 social stigma. This can also destabilise the society
Mass disruption of medical services	- Mass interruptions of appointments [34]. During the global pandemic online interruptions of appointments could disrupt the normal fabric of the society. - Disruption of vital medical facilities, for example, ventilators, which might be fatal. - Disruption of care and emergency services will lead to public unrest and instability.

Mass defacements of health websites	- Social disruption through the spread of propaganda – for example, in the case of the NHS websites where pictures of violence from Syria's war were uploaded on the sites [35]. - Unavailability of information, which might cause mass confusion and scare, especially in these times.

Table 2: Consequences of resourceful cyberwar against e-Health.

As indicated in the table above, the exploitation of e-Health with the resources and skills of cyberwar causes an impact on the physical domain, regardless of whether there is a global pandemic, which are felt on the civilian, military and government spheres.

While some strategic cyber-attacks directed towards e-Health, some of the attacks experienced are because of cyber-collateral damage [36]. For instance, the WannaCry cyber-attack which paralysed e-Health across the NHS (UK) resulting in cancellation of surgeries, hospital diversion of emergencies and unavailability of patient records in both England and Scotland [37]. Initial investigations indicate that the NHS was not the specific target [38] hence showing that cyber-collateral damage can have adverse effects on e-Health in the context of cyberwar. Further, according to Fritsch and Fischer-Hübner [39], "future Battlefield of Things will be the weaponization of civilian or dual-use infrastructure." This suggests that through interlinking of these infrastructures, the healthcare infrastructure can be caught in the crossfire thus having a destructive impact on an entire nation [10] as highlighted in Table 1 above.

Having established the impact of weaponizing eHealth in the context of cyberwar, there is urgent need for adequate measures to prevent the worst from happening. With a dramatic increase in the number of cyber-attacks, some of the leading healthcare organisations are now investing in cyber and information security after the WannaCry, for example the NHS (UK) and HHS (US). Granted that the healthcare sector implements existing laws (e.g. HIPAA [40]) or invest in current standards (e.g. ISO/IEC ISO/IEC 27001:2017 [41].) and frameworks (e.g. NIST-CSF or NIST-PF); would these be enough to prevent cyberwar in the context of eHealth? These laws, standards and frameworks are rather relevant, however, in the context of cyberwar and information security in healthcare, a number of them would come in handy. For example, ISO/IEC 27032:2012 that describes guidelines for cybersecurity provide controls for addressing cyber risks, including controls for cyber organised criminals [42] and ISO/IEC 27799:2016 that describes specific guidelines for information security management in health using ISO/IEC 27002 [43]. However, there needs to be implementation of other security measures to support the above. According to McGraw [3] one way to prevent this is to build security in the system that takes skilled and resourceful attackers with high levels of intent in consideration. Further, calculating possible risks by cyber-mapping all hardware and software within a critical infrastructure could protect critical infrastructure like e-Health from cyber threats [28]. In addition, improving the identification and management of highly advanced cyber incidents and attacks against critical infrastructures, for example, in the case of the European collaborative early warning system ECOSSIAN, [44] is also imperative in preventing the impact of cyberwar in e-Health.

References

1. Smith, A.C., et al., *Telehealth for global emergencies: Implications for coronavirus disease 2019 (COVID-19).* Journal of telemedicine and telecare, 2020: p. 1357633X20916567.
2. Bell, J., et al., *Tracesecure: Towards privacy preserving contact tracing.* arXiv preprint arXiv:2004.04059, 2020.
3. McGraw, G., *Cyber war is inevitable (unless we build security in).* Journal of Strategic Studies, 2013. **36**(1): p. 109-119.
4. Gaddi, A., F. Capello, and M. Manca, *eHealth, care and quality of life*. 2013: Springer.
5. Dixon, M.G., et al., *Contact tracing activities during the Ebola virus disease epidemic in Kindia and Faranah, Guinea, 2014.* Emerging infectious diseases, 2015. **21**(11): p. 2022.
6. Ossebaard, H.C. and L. Van Gemert-Pijnen, *eHealth and quality in health care: implementation time.* International journal for quality in health care, 2016. **28**(3): p. 415-419.
7. Coventry, L. and D. Branley, *Cybersecurity in healthcare: a narrative review of trends, threats and ways forward.* Maturitas, 2018. **113**: p. 48-52.
8. Erlingsdóttir, G. and H. Sandberg, *eHealth opportunities and challenges: a white paper.* 2016.
9. Kreps, G.L. and L. Neuhauser, *New directions in eHealth communication: opportunities and challenges.* Patient education and counseling, 2010. **78**(3): p. 329-336.
10. Walker-Roberts, S., M. Hammoudeh, and A. Dehghantanha, *A systematic review of the availability and efficacy of countermeasures to internal threats in healthcare critical infrastructure.* IEEE Access, 2018. **6**: p. 25167-25177.
11. Pappot, N., G.A. Taarnhøj, and H. Pappot, *Telemedicine and e-Health Solutions for COVID-19: Patients' Perspective.* Telemedicine and e-Health, 2020.
12. Bashshur, R., et al., *Telemedicine and the COVID-19 Pandemic, Lessons for the Future*. 2020, Mary Ann Liebert, Inc., publishers 140 Huguenot Street, 3rd Floor New ….
13. Cho, H., D. Ippolito, and Y.W. Yu, *Contact tracing mobile apps for COVID-19: Privacy considerations and related trade-offs.* arXiv preprint arXiv:2003.11511, 2020.
14. Williams, P.A. and A.J. Woodward, *Cybersecurity vulnerabilities in medical devices: a complex environment and multifaceted problem.* Medical Devices (Auckland, NZ), 2015. **8**: p. 305.
15. Liff, A.P., *Cyberwar: a new 'absolute weapon'? The proliferation of cyberwarfare capabilities and interstate war.* Journal of Strategic Studies, 2012. **35**(3): p. 401-428.
16. Sevis, K.N. and E. Seker. *Cyber warfare: terms, issues, laws and controversies*. in *2016 International Conference On Cyber Security And Protection Of Digital Services (Cyber Security)*. 2016. IEEE.
17. Martin, G., et al., *Cybersecurity and healthcare: how safe are we?* Bmj, 2017. **358**: p. j3179.
18. Raskar, R., et al., *Apps gone rogue: Maintaining personal privacy in an epidemic.* arXiv preprint arXiv:2003.08567, 2020.
19. Gross, M.L., D. Canetti, and I. Waismel-Manor, *The Psychological & Physiological Effects of Cyberwar.* Binary Bullets: The Ethics of Cyberwarfare, 2015: p. 157-76.
20. McRoberts, M., *Auckland woman 'creeped out' after restaurant worker uses her contact tracing details to hit on her*. 2020, Newshub.
21. Henrik, L., et al., *8300 mobiles tracked in hospitals and shelters (In Norwegian: 8300 mobiler sporet på sykehus og krisesentre).* 2020 [cited 22nd March 2020]; Available from: https://www.nrk.no/norge/mobilsporing_-8300-mobiler-sporet-pa-sykehus-og-krisesentre-1.15008085

22. BBC, *Coronavirus: Security flaws found in NHS contact-tracing app*. 2020.

23. Gollom, M., *LifeLabs cyberattack one of 'several wake-up calls' for e-health security and privacy*, in *CBC*. 2019.

24. Arquilla, J., *Twenty years of cyberwar.* Journal of Military Ethics, 2013. **12**(1): p. 80-87.

25. Warfare, J.L.C., *Journal of Law & Cyber Warfare Vol. 4:3 Winter 2015*. 2016: Lulu.com.

26. Kim;, M.J. and S. De, *A 'travel log' of the times in South Korea: Mapping the Movements of Coronavirus carriers*, in *The Washington Post*. 2020.

27. Szapranski, R., *A Theory of Information Warfare; Preparing for 2020*. 1995, AIR UNIV MAXWELL AFB AL.

28. Hughes, O. *Norway healthcare cyber-attack 'could be biggest of its kind'*. Digital Health 2018 [cited 11th March 2020]; Available from: https://www.digitalhealth.net/2018/01/norway-healthcare-cyber-attack-could-be-biggest/.

29. Corera, G., *Coronavirus: Cyber-spies hunt Covid-19 research, US and UK warn*. 2020.

30. Martin, G., et al., *When mobile becomes the enemy (In Norwegian: Når mobilen blir fienden)*. 2020, NRK. [cited 22nd May 2020]; Available from: https://www.nrk.no/norge/xl/norske-offiserer-og-soldater-avslort-av-mobilen-1.14890424

31. Trude, F., et al., *Revealed by mobile (In Norwegian: Avslørt av mobilen)*. 2020, NRK. [cited 22nd May 2020]; Available from: https://www.nrk.no/norge/xl/avslort-av-mobilen-1.14911685

32. BBC, *Wiggins and Froome medical records released by 'Russian hackers'.* 2016.

33. Fu, K. and J. Blum, *Controlling for cybersecurity risks of medical device software.* Communications of the ACM, 2013. **56**(10): p. 35-37.

34. Field, M., *WannaCry cyber attack cost the NHS £92m as 19,000 appointments cancelled.* 2018.

35. Sengupta, K., *Isis-linked hackers attack NHS websites to show gruesome Syrian civil war imag.* 2017.

36. Romanosky, S. and Z. Goldman, *Cyber collateral damage.* Procedia Computer Science, 2016. **95**(2): p. 10-17.

37. Mattei, T.A., *Privacy, confidentiality, and security of health care information: Lessons from the recent Wannacry cyberattack.* World neurosurgery, 2017. **104**: p. 972-974.

38. Morse, A., *Investigation: WannaCry cyber attack and the NHS.* London: National Audit Office. Accessed December, 2017. **31**: p. 2017.

39. Fritsch, L. and S. Fischer-Hübner, *Implications of Privacy & Security Research for the Upcoming Battlefield of Things.* Journal of Information Warfare, 2018. **17**(4): p. 72-87.

40. Assistance, H.C., *Summary of the hipaa privacy rule.* Office for Civil Rights, 2003.

41. Standardization, I.O.f., *ISO/IEC 27001: 2013: Information Technology--Security Techniques--Information Security Management Systems--Requirements*. 2013: International Organization for Standardization.

42. International Organization for Standardization, I.E.C., *ISO/IEC 27032: 2012–Information technology—Security techniques—Guidelines for cybersecurity.* 2012.

43. ISO, I., *27799: 2016 (en).* Health informatics â€" Information security management in health using ISO/IEC, 2016. **27002**.

44. Kaufmann, H., et al., *A structural design for a pan-European early warning system for critical infrastructures.* e & i Elektrotechnik und Informationstechnik, 2015. **132**(2): p. 117-121.