Cyberattacks are rewriting the ‘rules’ of modern warfare – we aren’t prepared for the consequences

Leiser, M.R.

Cyberattacks are rewriting the 'rules' of modern warfare – we aren't prepared for the consequences

Posted on May 24, 2019 by Mark Leiser in Public Law (https://leidenlawblog.nl/category/public-law)

Governments are becoming ever more reliant on digital technology, making them more vulnerable to cyberattacks. In 2007, Estonia was attacked by pro-Russian hackers who crippled government servers (https://ccdcoe.org/uploads/2018/10/Ottis2008_AnalysisOf2007FromTheInformationWarfarePerspective.pdf), causing havoc. Cyberattacks in Ukraine targeted the country's electricity grid (https://www.bbc.co.uk/news/av/technology-35686498/ukraine-power-hack-attacks-explained), and the Stuxnet malware (a 'virus') infected the uranium enrichment centre at Bushehr, Iran that could have led to a nuclear meltdown (https://foreignpolicy.com/2011/01/31/report-stuxnet-could-cause-iranian-chernobyl/). In the US, President Trump recently declared a "national emergency" (https://www.bbc.co.uk/news/world-us-canada-48289550?ocid=socialflow_facebook&ns_mchannel=social&ns_source=facebook&ns_campaign=bbcnews&fbclid=IwAR24dWmGc8vRQ6_ZuAuaeHOSNhQuSnO8 recognise the threat to US computer networks from "foreign adversaries".

Politically-motivated cyberattacks are becoming increasingly commonplace (https://www.csis.org/programs/cybersecurity-and-governance/technology-policy-program/other-projects-cybersecurity), but unlike traditional warfare between two or more states, cyberwarfare can be launched by groups of individuals (https://www.telegraph.co.uk/news/2019/02/18/chinese-iranian-hackers-increase-cyber-attacks-us/). On occasion, the state is actually caught in the crosshairs of competing hacking collectives (http://www.css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2018-04.pdf). This doesn't mean that states don't actively prepare for such attacks. British defence officials have said they're prepared to conduct cyberattacks against Moscow's power grid, should Russia decide to launch an offensive (https://qz.com/1416362/the-uk-war-games-cyberattacks-that-could-black-out-moscow/). In most cases, cyberwarfare operations have been conducted in the background, designed as scare tactics or displays of power. But the blending of traditional warfare and cyberwarfare seems inevitable and a recent incident added a new dimension.

How to respond to cyberattacks

Israeli Defence Forces bombed a building allegedly housing Hamas hackers, after they had attempted to, according to the IDF, attack "Israeli targets" online (https://twitter.com/IDF/status/1125066395010699264). This is the first time a cyberattack has been met with physical force by a state's military. But who is to blame and how should states respond when defending against cyberattacks?

Cyberattacks are a serious challenge for established laws of armed conflict. Determining the origin of an attack isn't impossible, but the process can take weeks (https://www.dni.gov/files/CTIIC/documents/ODNI_A_Guide_to_Cyber_Attribution.pdf). Even when the origin can be confirmed, it may be difficult to establish that a state was responsible. This is especially true when cyber operations could be perpetrated by hackers in other countries routing their attacks through different jurisdictions.

NATO experts have highlighted the issue in the Tallinn Manual on International Law Applicable to Cyberwarfare (http://csef.ru/media/articles/3990/3990.pdf). There is no consensus on whether a state is responsible for a cyberattack originating from its networks if it did not have explicit knowledge of the attack. Failure to take appropriate measures to prevent an attack by a host state could mean that the victim state is entitled to respond through proportionate use of force in self-defence. But if there's uncertainty around who is to blame for the attack, any justification for a counter-attack is diminished.

Even if the problem of attribution is resolved, a state's right to respond with force to a cyberattack would normally be prohibited. Article 2(4) of the UN Charter (http://legal.un.org/repertory/art2.shtml) protects the territorial integrity and political structures of states from attack. This can be lawfully bypassed if a state can claim they're defending themselves (http://legal.un.org/repertory/art51.shtml) against an "armed attack".

The International Court of Justice (https://www.icj-cij.org/files/case-related/70/070-19860627-JUD-01-00-EN.pdf) explains that: *It will be necessary to distinguish between the most grave forms of the use of force (those constituting an armed attack) from other less grave forms.*

So a cyberattack would justify force as self-defence if it could be considered an "armed attack". But is that possible? Only when the "scale" and "effect" of a cyberattack are comparable to an offline "armed attack", such as attacks that lead to deaths and widespread damage to infrastructure (https://www.zdnet.com/article/cyberwar-what-happens-when-a-nation-state-issued-cyber-attack-kills/). If so, self-defence is justified (http://csef.ru/media/articles/3990/3990.pdf).

But what about when a cyberattack has been successfully defended against? Then, its effects can only be guessed at. This makes deciding a proportional response even trickier. Physical force used as self-defence after the cyberattack has already been successfully defended against could be considered unnecessary and therefore, illegal. An exception, however, might be made for a pre-emptive defence against an imminent or possible attack (https://ccdcoe.org/uploads/2018/10/Art-06-Anticipatory-and-Preemptive-Self-Defense-in-Cyberspace-The-Challenge-of-Imminence.pdf).

When self-defence is considered reasonably necessary, the nature of the force permitted can vary. Proportionate counter-attacks with conventional military weapons can be acceptable responses to cyber operations (http://csef.ru/media/articles/3990/3990.pdf) under international law. These issues are only the start of the challenges posed by cyberwarfare, which will get more complicated as technology develops. The intellectual challenges this will generate are numerous, but we still can't help but be fearful. Societies face potentially devastating consequences from cyberwarfare as we become more reliant on information technologies and communication networks for everyday life – and we're only just starting to ask questions about it.

Note: This is an edited version of an article that originally appeared in The Conversation (https://theconversation.com/cyber-attacks-are-rewriting-the-rules-of-modern-warfare-and-we-arent-prepared-for-the-consequences-117043).

Add a Comment

Name (required)

E-mail (required)

Please enter the word you see in the image below (required)

test95

Your own avatar? Go to www.gravatar.com (http://www.gravatar.com)

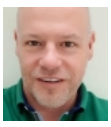
Remember me
Notify me by e-mail about comments

Submit

SHARE

(http://[illegible]
u=https[illegible]articles/cyberattacks-

AUTHORS



Mark Leiser

Assistant Professor (https://leidenlawblog.nl/contributors/mark-leiser)

TAGS

cyberattack (https://leidenlawblog.nl/tag/cyberattack) Cyberwar (https://leidenlawblog.nl/tag/Cyberwar)
public international law (https://leidenlawblog.nl/tag/public+international+law) terrorism (https://leidenlawblog.nl/tag/terrorism)

RELATED ARTICLES

Notes of caution on the UNSC resolution obliging states to change domestic criminal law (https://leidenlawblog.nl/articles/notes-of-caution-on-the-unsc-resolution-obliging-states-to-change-domestic)

Population of Holland also "marked for death"? (https://leidenlawblog.nl/articles/population-of-holland-also-marked-for-death)

Je suis concerned about political ostrichism (https://leidenlawblog.nl/articles/je-suis-concerned-about-political-ostrichism)

Leiden's tradition of moot courts (https://leidenlawblog.nl/articles/leidens-tradition-of-moot-courts)

How jihadists prepare their jihad (https://leidenlawblog.nl/articles/how-jihadists-prepare-their-jihad)

Stay Connected

- Twitter » (http://www.twitter.com/leidenlaw)
- Facebook » (http://www.facebook.com/leidenlawschool)
- LinkedIn » (http://www.linkedin.com/company/1009264?trk=tyah)
- YouTube » (http://www.youtube.com/LeidenLawSchool)
- Pinterest » (http://pinterest.com/leidenlaw/)

RSS

- Leiden Law Blog » (/feed)
- Criminal Law and Criminology » (/category/feed/criminal-law-and-criminology)
- Interdisciplinary Study of the Law » (/category/feed/interdisciplinary-study-of-the-law)
- Private Law » (/category/feed/private-law)
- Public Law » (/category/feed/public-law)
- Tax Law and Economics » (/category/feed/tax-law-and-economics)

Links

- Leiden Law School » (http://law.leiden.edu)
- Leiden University » (http://www.leiden.edu)
- NJBlog » (http://njblog.nl)
- Publiekrecht en politiek » (http://www.publiekrechtenpolitiek.nl)
- Juridisch PAO » (http://www.paoleiden.nl/cms2/)
- Disclaimer » (/disclaimer)