Dangerous Gaming: Cyber-Attacks, Air-Strikes and Twitter

https://www.e-ir.info/2019/09/23/dangerous-gaming-cyber-attacks-air-strikes-and-twitter/

ANDREW DWYER AND JANTJE SILOMON, SEP 23 2019

On May 5 2019, the Israeli Defense Forces (IDF) launched an air-strike against a building in the Gaza Strip. Air-strikes, missiles, and escalated rhetoric are not unusual in the region. However, this event was exceptional, it was a kinetic, asymmetric attack against an alleged cyber-attack, and one that was worryingly justified by dehumanising its targets through *gamified* logic. The IDF stated that it retaliated to a cyber-attack by Hamas' cyber operations amid a periodic flare-up in tensions and hostility between Israel and the group that governs the Palestinian territory. As only the second publicly confirmed response to a cyber-attack with kinetic force (after the first against Daesh by the United States in 2015), it is worthy of further reflection to explore the justification of these strikes against 'quasi-state' entities. However, unlike the first strike, the IDF's tweet of the air-strike deployed visual and linguistic cues that we believe prompt questions over our existing understanding and conceptualisation of cyber-attack retaliation. In this article, we explore how both gamification and kinetic action became bound together in a troubling, and justificatory, mix.

CLEARED FOR RELEASE: We thwarted an attempted Hamas cyber offensive against Israeli targets. Following our successful cyber defensive operation, we targeted a building where the Hamas cyber operatives work.

HamasCyberHQ.exe has been removed. pic.twitter.com/AhgKjiOqS7

— Israel Defense Forces (@IDF) May 5, 2019

By using gamified logics, the IDF served to normalise such action: positioning its air-strike on a plane similar to 'non-physical' cyber-attacks, transforming Hamas into inhuman targets. The tweet echoed an act of cleaning a *dirty*, malware-infected computer and was simultaneously reminiscent of gamers competing to remove or 'delete' one another, screened-off and partitioned from the realities and consequences of its air-strike. The language – "HamasCyberHQ.exe has been removed." – reduced Hamas to the level of 'kills' in gaming, whilst also seeking to justify an asymmetric response to a cyber-attack. So, how, and why, does this matter?

Focusing on the IDF's framing of the air-strike through gamification, we question how states asymmetrically respond to cyber-attacks. First, we examine how gamification obscured the operational difficulties of such a response, what this means, and how this informs discussions on cybersecurity. Second, we then consider how the reduction of life to nonhuman malware has become part of the process to justify an air strike. Finally, we suggest ways to think through the key implications of the air-strike and the IDF tweet in the setting of norms developed through engagements with quasi-state entities that come through the novel justification of strikes through gamified rhetoric. Therefore, in looking at the construction of new boundaries of *legitimate* action, we question what this attack means for the future of cyber and counter-cyber operations.

Gamifying Strikes

In comments published by Judah Gross (2019) in *The Times of Israel*, the Israeli state confirmed that it had prevented Hamas' cyber-attack prior to the subsequent air-strike. Whilst the planning and organisation of the kinetic response was likely highly complex, the IDF's portrayal was anything but. Instead, it was reminiscent of gaming's instant gratification, sidestepping inevitable operational and political complexities that are prevalent in assessing cyber-attacks, such as during attribution (Egloff and Wenger 2019).

The speed and simplicity of the tweet worked to reduce life, environments, and behaviour to the practice of computer gaming and strategy. Computer games, in particular, are often stylised, with time and space compressed and distorted, generating senses of distantiation and detachment between players and the subjects of game play. In similar ways, *cyberspace*, with its popular characterisations of ethereal 'non-physical' attributes, along with its supposed anonymity and boundlessness, is typically assumed to exhibit similar attributes to gaming (see Graham, 2013 for a broader perspective). In turn, actions taken *in* cyberspace have become understood as being less consequential than in conventional attacks. These elements came together in May 2019, when the IDF aligned an air-strike, through a tweet's language and visual cues, to imaginations of cyberspace and gaming where the IDF took on the role of the player, leaving Hamas as the game's subject.

Yet, games are not new to military doctrine and have become more prevalent in the period since the 'War on Terror' (Shaw, 2010; Power, 2007; Jensen, 2019). Gamification matters when it imbibes military action due to the precedents that it sets: in this case, to delimit who can *legitimately* respond to cyber-attacks and the treatment of those that they respond to. Both the air-strike, and its accompanying tweet presented in this article, positioned certain bodies and buildings as those to 'take-out'. They show how visual and linguistic rhetoric applied to cyber-attacks can put lives at the mercy of states. Yet, the explosiveness of an air-strike is withdrawn through this gamified imaginary where it instead seeks to flatten, render uncontroversial, and obscure responses to cyber-attacks – in order to justify an air-strike achieved through reducing its subjects to inhuman targets.

A simplicity must be constructed to sustain such action and perception, where an entire building can be demarcated in a red hue and neatly contained by a thick white borderline, depicting the alleged location of Hamas' cyber operations. It appears precise and clearly delineated, allowing for a strike with *surgical* precision, not unlike in similar justifications for drone warfare (Parks and Kaplan, 2017). Indeed drone warfare itself is conditioned by gaming, where it is practiced in pre-deployment training, leading to arguments, such as by Caroline Holmqvist (2013), that its potent and immersive qualities are critical to the operator's formation of reality.

As external observers, this apparent surgical precision and its allocation as such are hidden from us. Unlike in other domains, there is no independent 'physical' evidence we can use to corroborate the IDF's claim of Hamas' cyber-attack. We are left with nothing but the IDF's tweet. We do not know how much of the demarcated building was potentially used by Hamas. Could it have been as little as one floor, or even a single office? Furthermore, as cyber-attacks often use *civilian* infrastructures for nefarious activity, it makes distinguishing abnormal activities difficult to attribute. In short, we have no evidence to affirm Israel's claims of Hamas' cyber-attacks – which makes the study of its gamified rhetoric all the more important. It obscures even further the process and justification for launching a strike.

The active demarcation of a building is a complex exercise that can include analysing data, network monitoring, and perhaps even infiltrating Hamas' cyber operations. Yet, or maybe precisely because of such complexity and lack of certainty, a decision about the attribution of a cyber-attack to one building is ultimately a political act. At the same time, a general lack of public appreciation of attribution means gamification becomes a tool to surrender such complexities, instead providing a clear narrative that gives leeway to justify military and kinetic intervention.

The IDF, through their tweet, became the player of this 'game', relegating Hamas to less-than-real subjects that could be easily discovered, demarcated and destroyed. Going forward, such imaginaries between cyber-attacks, games, and air-strikes require further study. The images, language, decisions, and implications of this air-strike are not only relevant for understanding the politics behind responses to cyber-attacks, but how their imaginaries may indeed shape future conflicts themselves. No more so when there is a danger of no independent verification of events that are increasingly justified to publics through social media.

Reducing Life to Malware

Although some might argue that this event is a modern, and disturbing, extension of previous strategies, building upon arguments made by Derek Gregory in *The Colonial Present* (2004), there are worrying new developments. The growth of 'Twitter diplomacy' (Manor, 2019) has challenged conventional forms of state communication – that typically go beyond conveying 'facts'. Instead, they can be carefully crafted to deliver often subtle messages that both justify actions by states, offer insight into their strategic thinking, and sometimes merely provoke. The case of the IDF's tweet was no different: it shows the IDF are willing to use asymmetric force against cyber-attacks, are willing to engage in gamification to achieve these aims, and that attacking Israel is no different if you are behind a computer. Yet, this is unlikely to have been a deliberate strategy to invoke gamification and dehumanisation, which makes its presence even more concerning.

The tweet was infused with defining the abnormal, a disease – the 'pathologisation' – of warfare (McSorley, 2013) that was actively framed through gamification. By stating "HamasCyberHQ.exe has been removed", an asymmetry was formed that relegated Hamas as malware to be removed. Software relies, to a great extent, on 'executable' files, which often end in the format '.exe'. Malware is no different, resulting in 'anti-virus' programs seeking to remove malicious ones in order to keep computers and systems 'clean'. Gamers similarly seek to beat opponents, including using the language of deletion and removal, often joking, taunting or even 'flaming' (mocking) them in the process. Here, Hamas was to be *sterilised*, simply eliminated like nonhuman malware. A strong signal emerges through this gamified language: kinetic responses to computational infrastructure attacks on Israel are justified through pathological comparison. It also speaks to and justifies an air-strike with little connection to the visceral, physical realities of such responses to a generation accustomed to gaming culture through buildings in red hues and provocative language.

Quasi-State Asymmetry

So far, in contrast, most responses to attacks in the so-called 'cyber domain' (Kello, 2017) have remained non-kinetic, primarily attributing them to states and organisations – such as the United States' attribution of the 2014 Sony Pictures hack to North Korea (Cieply and Barnes, 2014; Haggard and Lindsay, 2015). More complex 'hybrid' interactions – such as in recent hostilities that have involved cyber-attacks 'below the threshold of armed conflict' between the United States and Iran (Barnes and Gibbons-Neff, 2019) – were not triggered by a cyber-attack, but have instead been incorporated as part of a suite of responses. Whilst it cannot be ascertained fully whether these cyber-attacks triggered kinetic responses, we can be confident that this case is fundamentally different to an explicit cyber-attack response as we discuss it in this article.

There have been substantial warnings provided by states against cyber-attacks however. In 2011 the United States unilaterally – and uniquely at the time – reserved the right to retaliate with military force against a cyber-attack (Department of Defense, USA, 2011, p.5). The subsequent Department of Defense's 2015 *Law of War Manual* stated that there 'is no legal requirement that the response in self-defense to a cyber armed attack take the form of a cyber action, as long as the response meets the requirements of necessity and proportionality' (2016, p.1017). Similarly, the first edition of the *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Schmitt, 2013), extensively used by the NATO alliance, has described the context in which a nation state may justify an armed response to a cyber-attack. This has recently been reaffirmed by its Secretary General, Jens Stoltenberg (2019), arguing that NATO is prepared to defend itself through the triggering of 'Article 5'.

The 2019 IDF air-strike is likewise not an isolated event. It followed a 2015 US drone strike that killed the then-head of Daesh's hacker groups, Junaid Hussain. Both strikes were against 'quasi-state' entities, in that they have or had claims over territory without being recognised as sovereign states. No actor has made explicit the boundaries of what would constitute a trigger for a kinetic response however – and even less so with quasi-state actors like Hamas. There are no public 'red lines' in terms of type of attack, its severity, systems targeted, or their consequences. Yet, as Max Smeets (2019) has recently argued on the *Lawfare* blog, within the United States, at least, '[t]he new challenge is to figure out what adversaries are allowed to do in cyberspace, not what they're *not* allowed to do'. He argues there are too many red lines because states are restricted to fewer 'competitive environments' – that are strategic to the

attacker but do not affect the (international) standing of the affected state. This presents something new that means we may see new areas of potential engagement opening-up with greater flexibility over what states try to do. Critical reflections such as over asymmetry are then all the more important as other places of conflict become more constricted and new spaces of conflict appear.

Deciding when a cyber-attack warrants an asymmetric response and the proportionality of this are broadly untested, and as such permits the exploration of the boundaries of when an air-strike can be used. There is work that seeks to address nonstate actors such as hacktivists, 'patriot' hackers, and cyber mercenaries that may provide useful avenues of exploration (Sklerov, 2009; Maurer, 2018). However, there is something distinctive about Hamas in the Gaza strip in that it has a clear territorial extent which makes an asymmetric air-strike 'easier'. As quasi-state groups control territory, but have no capacity to conduct air-strikes, they set a *potentially* lower threshold for kinetic responses to cyber-attacks. Due to being declared terrorist groups by those who launched air-strikes against them, they are perhaps more amenable to dehumanisation and gamification as experienced by Hamas. Thus, as there are only two publicly-known kinetic responses, we believe it is essential to more thoroughly theorise the activities of quasi-state actors in cybersecurity, how kinetic attacks may be 'trailed' in these spaces, and how gamification became such a central part of the IDF's air-strike.

Conclusion

The response to cyber-attacks is in a process of defining the doctrines, borders, and definitions of acceptable or normal behaviour. In this piece, we identified how quasi-state actors have been the first to be targeted by asymmetric air-strikes, which means these events should be given further attention in the formation of cyber-norms. Yet, perhaps most disturbingly, the IDF's tweet positions its air-strike against Hamas' cyber headquarters through gamified rhetoric, with simplified, clear-cut demarcations of activity and attribution.

Although there has been a history of gamification in warfare that has drawn boundaries between 'us' and 'them', and their mutual construction (Gregory, 2004; Barkawi and Laffey, 2006), there is a worrying mix in this case. It stems from a combination of elements that normalise new behaviour: the treatment of Hamas through Twitter diplomacy, gamification, and the demarcation of 'operational' space to target, all coalesced into the dehumanisation of both the targets and impacts of air-strikes – and in lowering (and potentially broadening this back to states) the threshold for this in the future.

In the IDF's case, the tweet rendered Hamas' cyber operations as 'characters' who, through gamification, became targets for expulsion akin to malware. As Hamas has no capacity to conduct air-strikes, they became, inadvertently, 'test-beds' for kinetic responses to cyber-attacks. Hence, we must keep an eye on these quasi-state engagements that appear distinct from state and nonstate responses that remain broadly symmetric. If we are to experience further movement between different 'domains', this is an area to critically attend to.

Furthermore, the lack of technical details about attribution then became partially justified through the gamified treatment of cyber-attacks, with a lack of independent verification, posing additional questions on how we can assess actions in response to cyber-attacks. This is not to say this was even a *deliberate* strategy of those who composed the tweet – and this makes this all the more insidious and important to reflect on, where justification and evidence are not provided as part of a 'normal' response to cyber-attacks. In this context, this second public kinetic response to cyber-attacks is critical as trends and norms set here could define and shape conflicts in the future. Although today all this has been focused on quasi-state entities, how this gamification dehumanises, diverts attention away from technical details and leaves independent verification near impossible sets an uneasy direction.

We would like to thank Ulrich Kühn and Benjamin Tallis for their suggestions and comments.

Bibliography

Barkawi, T. and Laffey, M., 2006. The postcolonial moment in security studies. *Review of International Studies*, 32(2), pp.329–352.

Barnes, J.E. and Gibbons-Neff, T., 2019. U.S. Carried Out Cyberattacks on Iran. *The New York Times*. [online] 22 Jun. Available at: https://www.nytimes.com/2019/06/22/us/politics/us-iran-cyber-attacks.html [Accessed 28 Jul. 2019]

Cieply, M. and Barnes, B., 2014. Sony Cyberattack, First a Nuisance, Swiftly Grew Into a Firestorm.*The New York Times*. [online] 30 Dec. Available at: https://www.nytimes.com/2014/12/31/business/media/sony-attack-first-a-nuisance-swiftly-grew-into-a-firestorm-.html [Accessed 28 Jul. 2019]

Department of Defense, USA, 2011. *Department of Defense Cyberspace Policy Report*. [online] p.12. Available at: https://nsarchive2.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-059.pdf [Accessed 28 Jul. 2019]

Egloff, F., J. and Wenger, A., 2019. *Public Attribution of Cyber Incidents*. [CSS Analyses in Security Policy] Zürich: CSS Zürich. Available at: https://web.archive.org/web/20190511085131/http://www.css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/CSSAnalyse244-EN.pdf

Graham, M., 2013. Geography/internet: ethereal alternate dimensions of cyberspace or grounded augmented realities? *The Geographical Journal*, 179(2), pp.177–182.

Gregory, D., 2004. *The Colonial Present: Afghanistan, Palestine, Iraq*. Blackwell Pub. Malden, MA.

Gross, J.A., 2019. IDF says it thwarted a Hamas cyber attack during weekend battle. *The Times of Israel*. [online] 5 May. Available at: https://www.timesofisrael.com/idf-says-it-thwarted-a-hamas-cyber-attack-during-weekend-battle/ [Accessed 5 Jun. 2019]

Haggard, S. and Lindsay, J.R., 2015. North Korea and the Sony hack: Exporting instability through cyberspace*East-West Center (EWC)*, East-West Center Asia Pacific Issues(117).

Holmqvist, C., 2013. Undoing war: War ontologies and the materiality of drone warfare. *Millennium*, 41(3), pp.535–552.

Jensen, B., 2019. *Welcome to Fight Club: Wargaming the Future*. [online] War on the Rocks. Available at: https://warontherocks.com/2019/01/welcome-to-fight-club-wargaming-the-future/ [Accessed 27 Jul. 2019]

Kello, L., 2017. *The Virtual Weapon and International Order*. New Haven: Yale University Press.

Manor, I., 2019. *The Digitalization of Public Diplomacy*. Palgrave Macmillan Series in Global Public Diplomacy. Palgrave Macmillan.

Maurer, T., 2018. *Cyber Mercenaries*. Cambridge, UK: Cambridge University Press.

McSorley, K., 2013. War and the Body. In: *War and the Body*. Routledge.pp.13–44.

Parks, L. and Kaplan, C. eds., 2017. *Life in the Age of Drone Warfare*. Durham, NC: Duke University Press.

Power, M., 2007. Digitized Virtuosity: Video War Games and Post-9/11 Cyber-Deterrence. *Security Dialogue*, 38(2), pp.271–288.

Schmitt, M.N., 2013. *Tallinn Manual on the International Law Applicable to Cyber Warfare* . Cambridge: Cambridge University Press.

Shaw, I.G.R., 2010. Playing war. *Social & Cultural Geography*, 11(8), pp.789–803.

Sklerov, M., 2009. Responding to international cyber attacks as acts of war. *Inside Cyber Warfare, J. Carr. O'Reilly*.

Smeets, M., 2019. *There Are Too Many Red Lines in Cyberspace* . [online] Lawfare. Available at: https://web.archive.org/web/20190726140149/https://www.lawfareblog.com/there-are-too-many-red-lines-cyberspace [Accessed 26 Jul. 2019]

Stoltenberg, J., 2019. Nato will defend itself. *Prospect Magazine*. [online] 27 Aug. Available at: https://www.prospectmagazine.co.uk/world/nato-will-defend-itself [Accessed 29 Aug. 2019]

US Department of Defense, 2016. *Law of War Manual*. [online] Office of General Counsel. Available at: https://dod.defense.gov/Portals/1/Documents/pubs/DoD%20Law%20of%20War%20Manual%20-%20June%202015%20Updated%20Dec%202016.pdf?ver=2016-12-13-172036-190

About the author:

Andrew Dwyer is a research affiliate at the Centre for Technology and Global Affairs and has recently submitted his doctoral thesis on malware, both at the University of Oxford. Recently, he was also a visiting fellow at the Collaborative Research Centre SFB/TRR 138, 'Dynamics of Security' in Germany.

Jantje Silomon is a researcher at the Institute for Peace Research and Security Policy at the University of Hamburg (IFSH) and has recently submitted a doctoral thesis in cybersecurity at the University of Oxford.