The new offensive cyber security: Strategically using asymmetrical tactics to promote information security

Received (in revised form): 16th December, 2021

Christopher Ott
Attorney, Rothwell Figg, USA

Chris Ott leverages his experience of more than 13 years at the U.S. Department of Justice (DOJ), including successfully litigating complex data security matters, conducting hundreds of investigations and winning dozens of appeals' Chris, CIPP/US, works with Rothwell Figg clients on disputes, investigations and strategy relating to data security, privacy, blockchain and artificial intelligence (AI) issues. Chris has been the lead attorney on hundreds of matters involving the intersection between white collar matters (accounting, securities, money laundering) and cybercrimes (from international criminal gangs to state actors). Prior to entering private practice, Chris held various influential positions at DOJ. In these roles, he investigated and charged the largest known computer hacking and securities fraud scheme and the hack of Yahoo by Russian intelligence operatives, the largest data breach in history, as well as driving other notable cyber investigations and white-collar investigations. He led multi-attorney and multi-agency law enforcement and regulatory investigations into securities fraud, wire fraud, hacking, health care fraud, privacy intrusions, money laundering, money transmitting and Foreign Corrupt Practices Act (FCPA) violations. He consulted extensively with the intelligence community while advancing cyber investigations. Chris also acted as Senior Trial Counsel of the Business and Securities Fraud Unit in the Eastern District of New York (EDNY), Assistant United States Attorney in the Business and Securities Fraud Unit in EDNY and Assistant United States Attorney in the Southern District of California (SDCA). Throughout his time at the DOJ he won multiple awards, including the 2018 Assistant Attorney General's Award for Excellence.

Rothwell Figg, 607 14th Street, N.W., Suite 800, Washington, DC 20005, USA
Tel: +1 202-783-6040; E-mail: COtt@rothwellfigg.com

Abstract Since the very first hack, cyber security professionals have sought to take the fight back to the hackers. Offensive cyber security operations usually focus upon proactive technical attacks on hackers to disrupt their operations and deter future attacks, and there are currently efforts by governments to expand these capabilities. Cyber security professionals are locked in an unfair, asymmetrical conflict with hackers, but they need not confine their thinking to historical rules of engagement. This paper briefly traces the theories of asymmetrical warfare in the 21st century, including its cyber security dimensions, to explore how companies and cyber security decision makers can learn from the lessons of the past while changing the rules of the conflict in their favour.

KEYWORDS: cyber security, asymmetrical warfare, offensive cyber security, active cyber security defence, cyber security theories

INTRODUCTION

Since the very first hack, cyber security professionals have sought to take the fight back to the hackers. Offensive cyber security possesses the tactical advantage of stopping or pre-empting cyber attacks before they impair target systems or penetrate cyber defences. These offensive cyber security operations

usually focus upon proactive technical attacks on hackers to cripple or disrupt their operations and deter future attacks. Indeed, there are current efforts by governments to expand these technical offensive cyber security capabilities.[1] Conceptually, this decision to engage in cyberwarfare in the purely technical realm makes intuitive sense: counter a technical attack with a proportional cyberattack; however, cyber security professionals need not confine their thinking to historical rules of engagement.

In the 21st century, decision makers at all levels of public life have become increasingly aware that they must engage in asymmetrical or hybrid warfare.[2] Asymmetrical warfare refers to unconventional strategies and tactics adopted by a force when the capabilities of the belligerent powers are not simply unequal but are so significantly different that they cannot make the same sorts of attack on each other.[3] Asymmetrical warfare can embrace a number of unconventional warfare tactics — indeed, some definitions embrace guerrilla and terrorist tactics.[4] For our purposes, however, we will focus on the tactics often referred to as the 'Gerasimov doctrine', which combines military, technological, information, diplomatic, economic, cultural and other tactics for the purpose of achieving strategic goals.[5] The approach contemplates a range of actors and tools, as well as conventional and asymmetric military means.

The Gerasimov doctrine builds a framework for these new tools and declares that non-military tactics are not auxiliary to the use of force but the preferred way to win. For example, Russia resorted to hybrid warfare in its campaign against Georgia, including cyberattacks, disinformation and the use of proxies in the breakaway South Ossetia region in the run-up to the war.[6] Those types of asymmetric attacks change the terms of engagement and often mandate asymmetric defences.[7] That realisation is dawning upon Western leaders on the sociopolitical stage. The same principles should be applied to cyber security. Too often, cyber security defenders fail to realise that they are locked in asymmetrical conflict.

To paraphrase C.A. Primmermanof the Defense Threat Reduction Agency (DTRA), a threat is asymmetrical if a business cannot do the same action back to them.[8] Although there is an urge to 'hack back', a business possesses a very limited ability to utilise the precise same tactics back at the threat actor. After all, one cannot deploy ransomware back at the gang of hackers. Therefore, cyber security threats provide classic asymmetric threats. The question is what can be done to respond to these asymmetrical threats.

In the overt warfare context, academics have championed the use of the legal system to counter asymmetrical warfare.[9] This provides an interesting idea: if the asymmetric aggressors gain the advantage by deploying tactics that cannot be deployed by the victims, perhaps the victims should use legal tools that are unavailable to the bad guys. This leads us back to legal options. Locked in an asymmetrical conflict with cybercriminals, businesses should explore deploying tactical assets that are generally unavailable to criminal networks: the legal system.

Through the strategic deployment of asymmetrical tactics, businesses have the opportunity to drive action via offensive litigation, not merely responding to threats. Sometimes, this involves threatened or actual suits against vendors who place a business's information security at risk. Other times, a more active option is explored. No matter what form it takes, more and more companies are making public lawsuits out of their private fights against information security bad actors. The nature of these fights often depends on the nature of one's own company.

THE DANGERS OF HACKING BACK

While we have focused on asymmetrical responses to cyber security threats, we should also discuss approaches that involve

launching a cyberattack against adversaries to disrupt or cripple their operations and to deter their future attacks. This approach is sometimes referred to as 'hacking back' and targets threat actors that have been identified as launching cyberattacks against you or your organisation.

There is a significant initial hurdle to any attempt to 'hack back'. Most importantly, most hack-back techniques would violate the Computer Fraud and Abuse Act (CFAA) and analogous state statutes. This is a major hurdle to most hack-back strategies — after all, your business would open itself to criminal and civil penalties. There is currently proposed legislation that would permit certain hack-back techniques; however, that bill has been roundly criticised and does not appear close to passing at time of writing.[10]

Even forgetting its dubious legality, the largest problem with any hack-back strategy is the risk of missing your shot. To begin, the bad guys may be misusing otherwise legitimate resources to effectuate their hacks. Targeting something like misused Amazon Web Services (AWS) architecture for vigilante hacking would be a terrible idea. Moreover, hacking can have huge, unintended spill-over effects. A fully fledged cyber offensive could inflict devastation comparable in scale to a conventional war or natural disaster. Targeting a botnet and taking down a school's notification system would not be a good outcome for anyone. Therefore, it makes sense to focus on asymmetrical strategies other than hacking back.

PLATFORM ABUSES AND DOMESTIC BAD ACTORS

On 27th February, 2020, Facebook filed a federal lawsuit in a California court against OneAudience, a New Jersey-based data analytics company.[11] Facebook alleged that OneAudience improperly accessed and collected user data from Facebook and other social media companies by paying app developers to install a malicious software development kit (SDK) in their apps. On 11th March, 2021, Facebook announced a settlement whereby OneAudience agreed to an audit, a permanent injunction banning them from using Facebook in the future and engaging in the challenged practices, as well as the payment of monetary damages.

The OneAudience case was notable for many reasons. One of the most important is its success. In settling, OneAudience agreed to everything and paid damages. Clearly, these types of offensive suits can have tremendous success.

A second notable detail is how Facebook learned of and acted upon these abuses. Security researchers notified Facebook of OneAudience's behaviour as part of their data abuse bounty programme. Facebook then took enforcement measures against OneAudience, including disabling apps, sending the company a cease-and-desist letter and requesting their participation in an audit, as required by their policies. When OneAudience declined to cooperate, Facebook brought a lawsuit.

The third detail lies in the legal theories that Facebook pursued in their lawsuit.[12] First, they alleged a breach of contract following breaches of the terms of service and the platform policies. Any business whose terms and policies are violated by cybercriminals could conceivably articulate the same claim. These contact claims constitute an asymmetric response to OneAudience's excesses, which is laudable.

Facebook also sued OneAudience for violations of the Computer Fraud and Abuse Act (CFAA)[13] and California Penal Code Section 506.[14] Both the CFAA and Section 506 interestingly provide both criminal and private civil penalties for most hacking activities. So, a business could find itself pursuing a case that largely mirrored a criminal hacking case. These hybrid statutes provide an important lever for businesses that seek asymmetrical responses. Any case

brought under the CFAA (or similar hybrid statutes) will necessarily draw the interest of law enforcement officials. The bad actors, faced with such a suit, are encouraged to either quickly come to terms or face overt criminal investigations. In the face of such hybridised threats, many bad actors will seek a quick settlement, as OneAudience did.

A recent US Supreme Court case has narrowed the scope of civil cases under the CFAA.[15] This narrowing notably removed the ability to seek relief against employees or former employees who may have been authorised to access company data for certain purposes, but who improperly accessed the same data for an improper purpose. This narrowed law, however, should not construct the ability to seek relief when the access was fraudulent in the first instance, which is almost always the case in hacking cases. Therefore the CFAA should remain a vital asymmetrical tool.

A fourth detail about the OneAudience case provides important information about coalition actions against bad actors. Facebook learned of the malware deployment from third parties and expressly brought the suit for the benefit of third-party companies that were negatively affected. Businesses therefore can, in the right circumstances, use the resources of a major tech player such as Facebook, Microsoft or Google — all of whom have demonstrated interest in offensive cyber security litigation — to bring the case on your behalf. Those David and Goliath partnerships can be delicate, fraught and hard to control, but the upside is notable.

Obviously, these specific types of lawsuit are best brought against a bad actor over whom a court will have jurisdiction, as in the case of suing the New Jersey-based OneAudience in San Francisco. Moreover, these types of lawsuit can be intuitive where they can identify a company to sue. Many of these hackers, however, are spread throughout the world and have informal business structures. While those differences would appear to cause problems, all is not lost.

OFFENSIVE LITIGATION AGAINST FOREIGN HACKERS

On 29th June, 2021, plaintiff Facebook filed a fraud lawsuit against Vietnamese hackers in the US District Court for the Northern District of California due to an 'account takeover attack'. The complaint alleged:

> 'Beginning no later than October 2020 and continuing to at least June 2021, Defendants took control of user accounts on Facebook in order to run millions of dollars of ads. Defendants misused cookies to take control of the accounts, a technique known as "session or cookie theft", and targeted employees of advertising and marketing agencies, which had access to large corporate ad accounts.'

Facebook further alleged:

> 'Defendants first misled the victims into self-compromising their user accounts by causing them to install a mobile app from the Google Play Store deceptively called "Ad Manager for Facebook" that was not actually affiliated with Facebook. When victims installed the malicious app, they shared their Facebook account login credentials and made accessible other information, which Defendants then used to access their Facebook accounts and run ads without the victims' knowledge or consent.'

Facebook brought this action (as with OneAudience) for violations of California Comprehensive Computer Data Access and Fraud Act, Cal. Penal Code § 502, the CFAA and breach of contract. While it is too early to expect a resolution, Facebook appears to have no reservations about bringing suit against Vietnamese hackers in US courts.

It is also worth noting that even shadowy hackers may have a domestic presence that can be legally challenged. Recent reporting has revealed that ransomware gangs recruit their tech talent using front companies.[16] Such a front company could be righteously sued. Similarly, if the hackers are also involved in managing the semi-legitimate aspects of their hosting services, those companies can also be sued under similar theories to those deployed by Facebook and Microsoft.

LAWSUITS ATTACKING HACKING INFRASTRUCTURE

Even if hackers are completely unreachable by legal process, the cyber infrastructure that they deploy will still be subject to legal attack. For example, it is not uncommon for a spear phishing campaign to utilise domains that are managed and administered in the US. Hackers often reuse domains in multiple hacking campaigns. In a prominent example, the infamous Solarwinds hack reutilised a complex web of domains to control their hack.[17] These domains are critical pieces of their ability to conduct these hacks.

On 27th December, 2019, the US District Court for the Eastern District of Virginia unsealed documents detailing a lawsuit that Microsoft brought to disrupt cyberattacks from a North Korean threat group.[18] The lawsuit resulted in a court order enabling Microsoft, a private entity, to take control of 50 domains that the group uses to conduct its operations. With this action, the sites could no longer be used to execute attacks.

Microsoft's Digital Crimes Unit (DCU) and the Microsoft Threat Intelligence Center (MSTIC) monitored the group's activities to establish and operate a network of websites, domains and Internet-connected computers. This network was used to target victims[19] and then compromise their online accounts, infect their computers, compromise the security of their networks and steal sensitive information. Based on victim information, the targets included government employees, think tanks, university staff members, members of organisations focused on world peace and human rights, and individuals who work on nuclear proliferation issues. Most targets were based in the US, as well as Japan and South Korea.

This was the fourth nation-state activity group against which Microsoft has filed similar legal actions to take down malicious domain infrastructure. Previous disruptions have targeted Barium, operating from China, Strontium, operating from Russia and Phosphorus, operating from Iran. These actions resulted in the takedown of hundreds of domains.

ASYMMETRIC CYBER SECURITY IS NOT A ONE-SIZE-FITS-ALL REMEDY

There is a reason why the above examples prominently involve Facebook and Microsoft. Those companies are so large and so complex that their interests often parallel or otherwise coincide with nation states. As such, their decisional calculus will be different from even other large companies which face hacking threats and could be sued. That said, their efforts are instructive to companies of all sizes.

Other high-profile cyber security matters are illustrative of how infrastructure could be attacked by smaller companies. In December 2016, Human Security, then known as White Ops, a US cyber security company that specialises in digital ad fraud and botnets, published a report that pinpointed much of the technical information about the 3ve operation and its financial damages.[20] Methbot, White Ops concluded, 'was the largest and most profitable advertising fraud operation to strike digital advertising to date'. A sizable number of the servers that the Methbot operation rented and utilised were owned and maintained by companies affiliated with XBT Holding S.A., which has operations in Dallas, Texas. Among its web-hosting domains are DDoS.com,

1-800-HOSTING and SecureVPN.com. A series of reports by the *Miami Herald* documented how major web viruses have spread via XBT's infrastructure.[21] The Methbot infrastructure was ultimately dismantled through a combination of law enforcement and private sector cooperation.[22] This was not an isolated approach.

To combat the 3ve, White Ops and Google led a broad alliance of nearly 20 companies spanning ad tech, security and Internet infrastructure.[23] This alliance shared information, cooperated with law enforcement and leveraged their own cyber security assets to dismantle the infrastructure. The White Ops/Human Security approach is an interesting exercise of what we could call the public/private partnership model. They utilised the resources of the larger Google and the tools of the US government to achieve their goals.

The exact ratios of each participant's activity in such a partnership can be determined on a case-by-case basis. Sometimes, it would make sense to rely more heavily on the larger partner's resources. For example, a hacking campaign's back can be broken via the release of targeted Microsoft updates.[24] Other times, the government's resources could be best suited for combatting a state-sponsored hacking campaign. Sometimes, however, the smaller company can offer quite a bit, as it appears can be done for the monitoring of the 3ve advertising fraud traffic by the botnet. Other times, it may be that a narrower, purely private partnership can accomplish the cyber security goals. No matter the distribution of efforts, this type of coalition building can form a classic asymmetric threat to the hackers. After all, cooperation is not a tool that they have.

BENEFITS AND RISKS OF OFFENSIVE LITIGATION AS AN ASYMMETRICAL TOOL

Overt litigation has distinct benefits. The first is control. If a business initiates a lawsuit, then that company gets to determine who to sue, when to sue, what remedies to seek (including damages and injunctive relief) and when to stop pursuing the case. That control can be very important.

The second benefit is the remedies themselves. Successful litigation can result in nearly immediate injunctive relief. That injunctive relief, which would take the form of a court order, would result in immediate relief from the use of, for example, certain US-based hacking infrastructure. In that circumstance, you could see affirmative results within days. In a longer time period, there is an opportunity to obtain damages from the bad actors or their partners. Those damages will arrive at a longer timeline than injunctive relief but — to paraphrase Eddie Felson — money won is twice as sweet as money earned.[25]

The third benefit is built-in transparency. By making allegations in court, a company is expressly stating that it has the proof. This express imprimatur makes it clear how strongly a company will stand behind its allegations. This transparency, you may recall, is one of the key features of how to respond to asymmetrical warfare. Asymmetrical warfare can benefit from the same values.

The fourth benefit is that the public can learn about your efforts. Not all cyber security efforts need to be cloaked in darkness. Court proceedings are, by default, public matters. Depending on a company's field, there is real value to making your offensive efforts a matter of public record. Obviously, Facebook, Microsoft and Google identified a benefit to publicising their offensive cyber security efforts; however, even smaller companies like White Ops/Human Security have raised their profile by making their efforts a matter of public record. A lawsuit can serve that purpose.

The downsides of litigation begin with cost. A business will have to have internalised the net benefits of the litigation. Until it has done so, the litigation may feel like pure cost. Also, the transparency and the

publicity of such a move must be considered. Some businesses do not want to invite public scrutiny of such moves. For the right companies, however, the publicity will be golden.

THIRD PARTY LITIGATION, WHISTLEBLOWING AND THE FUTURE OF ASYMMETRICAL CYBER SECURITY

New asymmetrical cyber security tools are coming all the time. The US Department of Justice has said it will launch civil legal actions against federal contractors if they fail to report cyberattacks or data breaches.[26] The Civil Cyber-Fraud Initiative, introduced by Deputy Attorney General Lisa O. Monaco on 6th October, 2021, will leverage the existing False Claims Act (FCA) to 'pursue cyber security-related fraud by government contractors and grant recipients'.

The initiative will hold entities, such as federal contractors or individuals, accountable when they put US cyber infrastructure at risk by knowingly providing flawed cyber security products or services. Similarly, government contractors now also face penalties for 'violating obligations' to monitor and report cyber security incidents and breaches. This may seem interesting but irrelevant; however, the details provide an interesting tool: the Civil Cyber-Fraud Initiative will utilise the False Claims Act (FCA).

The FCA is the government's primary civil tool to redress false claims for federal funds and property involving government programmes and operations. The act includes a unique whistleblower provision, which allows private parties to assist the government in identifying and pursuing fraudulent conduct and to share in any recovery, and protects whistleblowers who raise these violations and failures from retaliation. Therefore, this new type of cyber security litigation will have costs borne by the government and special whistleblower protections.

While the Civil Cyber-Fraud Initiative may not apply to every company, its advent further legitimises the use of asymmetrical cyber security tools. Smart and agile businesses will begin exploring those options now.

CONCLUSION

Asymmetrical warfare has taken over global conflicts, weaponising civil lawsuits, news cycles and social media in massive conflicts without firing a bullet. Cyber security decision makers should adopt the lessons of asymmetrical warfare and utilise an all-tools strategy to respond in kind.

References

1. Malnick, E. (October 2021), 'Britain to carry our "offensive" cyber attacks from new £5bn digital warfare centre', *Telegraph*, available at https://www.telegraph.co.uk/politics/2021/10/02/britain-capable-launching-offensive-cyber-attacks-against-russia/ (accessed 16th December, 2021).
2. Tromblay, D. E. (August 2016), 'The Intelligence Studies Essay: "Hybrid Warfare" at Home: Asymmetric Tactics Are Not Just Used in Ukraine, They Are Employed Against the United States, and Have Been for Quite Some Time', LawFare, available at https://www.lawfareblog.com/intelligence-studies-essay-hybrid-warfare-home-asymmetric-tactics-are-not-just-used-ukraine-they-are (accessed 16th December, 2021).
3. Sexton, E., 'Asymmetrical warfare', Britannica, available at https://www.britannica.com/topic/asymmetrical-warfare (accessed 16th December, 2021).
4. Rand Corporation (May 2020), 'Asymmetric warfare', available at https://www.rand.org/topics/asymmetric-warfare.html (accessed 16th December, 2021).
5. See McKew, M. K. (September/October 2017), 'The Gerasimov Doctrine', available at https://www.politico.com/magazine/story/2017/09/05/gerasimov-doctrine-russia-foreign-policy-215538/; but see also — criticizing the use of the term, Galeotti, M. (March 2018), 'I'm Sorry for Creating the "Gerasimov Doctrine"', Foreign Policy, available at https://foreignpolicy.com/2018/03/05/im-sorry-for-creating-the-gerasimov-doctrine/ (both accessed 16th December, 2021).
6. Nilsson, N. (January 2018), 'Russian Hybrid Tactics in Georgia', Silk Road, available at https://silkroadstudies.org/resources/pdf/SilkRoadPapers/2018_01_Nilsson_Hybrid.pdf (accessed 16th December, 2021).

7. Jones, S. G. (February 2021), 'The Future of Competition: U.S. Adversaries and the Growth of Irregular Warfare', CSIS, available at https://www.csis.org/analysis/future-competition-us-adversaries-and-growth-irregular-warfare (accessed 16th December, 2021).
8. As stated by Chris Mark 'Adversary A would attack Business A by doing X […] If we transform this statement by projecting the adversary's actions onto the business, we get […]. Business A would (or could) respond to Adversary A's attack by doing X. Now we have the simple conclusion that statement (1) represents an asymmetric action if statement (2) is false, and it represents a symmetric action if statement (2) is true', (May 2021), 'Asymmetrical threats in cybersecurity', AT&T Business, available at https://cybersecurity.att.com/blogs/security-essentials/asymmetrical-threats-in-cybersecurity (accessed 16th December, 2021).
9. Heinegg, W. H. von, 'Asymmetric Warfare: How to Respond?', *International Law Studies*, Vol. 87, available at https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?referer=&httpsredir=1&article=1089&context=ils (accessed 16th December, 2021).
10. Rempe, K. J. (January 2021), 'The "Hack Back" Bill: A Necessary Defense Mechanism, or a Precipitous Disaster?', Wake Forest Law Review, available at http://www.wakeforestlawreview.com/2021/01/the-hack-back-bill-a-necessary-defense-mechanism-or-a-precipitous-disaster/ (accessed 16th December, 2021).
11. Romero, J. (March 2021 [February 2020]), 'Taking Action Against Platform Abuse', Meta, available at https://about.fb.com/news/2020/02/taking-action-against-platform-abuse/ (accessed 16th December, 2021).
12. *Facebook, Inc. v OneAudience LLC*, Case 3:20-cv-01461 (27th February 2020), United States District Court, California, available at https://www.documentcloud.org/documents/6788988-Facebook-v-OneAudience-File-Stamped-Complaint.html (accessed 16th December, 2021).
13. Cornell Law School, '18 U.S. Code § 1030 – Fraud and related activity in connection with computers', available at https://www.law.cornell.edu/uscode/text/18/1030 (accessed 16th December, 2021).
14. FindLaw (January 2019), 'California Code, Penal Code – PEN § 506', available at https://codes.findlaw.com/ca/penal-code/pen-sect-506.html (accessed 16th December, 2021).
15. Bluestone, L., Burns, G. and Szabo, K. (June 2021), 'Supreme Court Narrows Liability Under the Computer Fraud and Abuse Act', JDSupra, available at https://www.jdsupra.com/legalnews/supreme-court-narrows-liability-under-9423793/ (accessed 16th December, 2021).
16. MacMillan, R. (October 2021), 'Ransomware Gang Masquerades as Real Company to Recruit Rich Talent', *Wall Street Journal*, available at https://www.wsj.com/articles/ransomware-gang-masquerades-as-real-company-to-recruit-tech-talent-11634819400 (accessed 16th December, 2021).
17. Slowik, J. (December 2020), 'Unraveling Network Infrastructure Linked to the SolarWinds Hack', DomainTools, available at https://www.domaintools.com/resources/blog/unraveling-network-infrastructure-linked-to-the-solarwinds-hack (accessed 16th December, 2021).
18. Burt, T. (December 2019), 'Microsoft takes court action against fourth nation-state cybercrime group', Microsoft, available at https://blogs.microsoft.com/on-the-issues/2019/12/30/microsoft-court-action-against-nation-state-cybercrime/ (accessed 16th December, 2021).
19. Per Microsoft, this group succeeded, in part, '[b]y gathering information about the targeted individuals from social media, public personnel directories from organizations the individual is involved with and other public sources, Thallium is able to craft a personalized spear-phishing email in a way that gives the email credibility to the target. As seen in the sample spear-phishing email below, the content is designed to appear legitimate, but closer review shows that Thallium has spoofed the sender by combining the letters "r" and "n" to appear as the first letter "m" in "microsoft.com".'
20. WhiteOps (November 2018), 'WhiteOps, Google Dismantle Massive Online Fraud Operations Named "3ve"', available at https://www.humansecurity.com/newsroom/3ve-google-whiteops-online-fraud (accessed 16th December, 2021).
21. *Miami Herald* (June 2020), 'Christopher Steele of Steele dossier fames scores win over Russian oligarchs in court', available at https://www.miamiherald.com/news/politics-government/article243646362.html (accessed 16th December, 2021).
22. WhiteOps, ref. 20, see above.
23. Sheridan, K. (November 2018), 'Google, WhiteOps, Industry Players Dismantle 3ve Ad Fraud Operation', DarkReading, available at https://www.darkreading.com/threat-intelligence/google-white-ops-industry-players-dismantle-3ve-ad-fraud-operation (accessed 16th December, 2021).
24. Krebs on Security (March 2021), 'Microsoft: Chinese Cyberspies Used 4 Exchange Server Flaws to Plunder Emails', available at https://krebsonsecurity.com/2021/03/microsoft-chinese-cyberspies-used-4-exchange-server-flaws-to-plunder-emails/ (accessed 16th December, 2021).
25. IMDb, 'Paul Newman: Eddie', available at https://www.imdb.com/title/tt0090863/characters/nm0000056 (accessed 16th December, 2021).
26. The US Department of Justice (October 2021), 'Deputy Attorney Lisa O. Monaco Announces New Civil Cyber-Fraud Initiative', available at https://www.justice.gov/opa/pr/deputy-attorney-general-lisa-o-monaco-announces-new-civil-cyber-fraud-initiative (accessed 16th December, 2021).