HP WOLF SECURITY

NATION STATES, CYBERCONFLICT AND THE WEB OF PROFIT

BY DR. MICHAEL MCGUIRE, SENIOR LECTURER IN CRIMINOLOGY, UNIVERSITY OF SURREY

TABLE OF CONTENTS

FOREWORD FROM IAN PRATT,

Global Head of Security for Personal Systems, HP Inc.

The world of Nation State cyberconflict and cyberespionage is covert by nature. Finding evidence of how such players operate, what tools they use, what motivates them and how they gain supremacy has always been challenging. Therefore, we are excited to share this study from Dr. Michael McGuire, Senior Lecturer of Criminology at the University of Surrey in the UK, which shines a light into how the Nation State cybersphere is evolving.

Over the past year, Nation States have become increasingly bold in their use of cyber capabilities to bolster sovereign interests – for example, the recent SolarWinds supply chain attack is widely considered to be the most sophisticated Nation State attack since Stuxnet. There have also been several brazen attempts to steal intellectual property around Covid-19 vaccine development. This has brought the issue of Nation State interference out of the shadows and into the limelight, making this report even more timely.

As Dr. McGuire's study shows, this escalation in tensions could have easily been foretold. There has been a steady upwards trajectory in the severity, openness and variety of Nation State cyber activities over the past twenty years. This has been driven, in part, by the widening use of cyber to support traditional military and intelligence goals – including surveillance, espionage, disruption and destruction. Worryingly, the report also highlights that the cyber and physical worlds are now colliding with potentially disastrous consequences, through cyberattacks against critical infrastructure.

The intersection between Nation States and the cybercrime economy – also known as 'The Web of Profit' – is a particularly interesting development. Nation States are knowingly engaging with this Web of Profit – buying and trading in tools, data, services, and talent – to further their strategic interests or 'keep their hands clean' of misdeeds by using proxies for cyberattacks. Equally, tools developed by Nation States are also making their way onto the cyber black market – tools like EternalBlue, the notorious exploit that was used by the WannaCry hackers in 2017.

In my role as Global Head of Security for Personal Systems, I see three key takeaways from the report:

01 **The innocent are being caught in the crossfire:** Nation State conflict does not exist in a vacuum – businesses and individuals alike are being sucked into its sphere either as direct targets (e.g. research facilities developing vaccines) or as stepping stones to bigger targets (e.g. SolarWinds supply chain hack).

02 **A cyber-treaty won't be coming overnight:** As a comparatively new area of international relations, there are fewer 'rules' and far more grey areas – for example, blurred lines between Advanced Persistent Threat (APT) groups and Nation States. While there is hope we will one day come to an agreement on cyberwarfare and cyberweapons, today there is very little in place that can stem the tide.

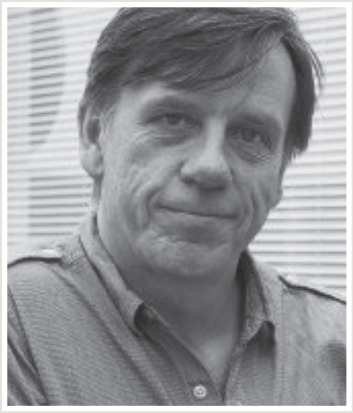
03 **The endpoint remains the most common point of infection:** Individuals and businesses alike need to protect themselves; the best way to do this is by defending the endpoint. Whether it's social engineering and phishing being used to infect targets, steal credentials and maintain persistence, the endpoint is the number one point of infection for all breaches.

As the severity, sophistication, scale and scope of Nation State activity continues to increase, we need to reinvent security to stay ahead. This will require a more robust endpoint security architecture built on zero trust principles of fine-grained segmentation coupled with least privilege access control. We are all in the crossfire now, so it's critical that every business does what it can to protect itself and its wider network.

...the recent SolarWinds supply chain attack is widely considered to be the most sophisticated Nation State attack since Stuxnet.

There has been a steady upwards trajectory in the severity, openness and variety of Nation State cyber activities over the past twenty years.

As the severity, sophistication, scale and scope of Nation State activity continues to increase, we need to reinvent security to stay ahead.



EXECUTIVE SUMMARY FROM DR. MICHAEL MCGUIRE,

Senior Lecturer in Criminology, University of Surrey

The strategies set out in the famous text ***The Art of War***, by the ancient Chinese military thinker Sun Tzu, offer rich insights into the novel kinds of struggle unfolding in cyberspace between Nation States. His prescient suggestion that a defining characteristic of the struggle here appears to be, to "subdue the enemy's troops without any fighting" is particularly pertinent.

While Nation State subterfuge is by its nature a notoriously opaque area of research due to high levels of classification, this study offers unique insight and informal reports acquired from publicly available information (such as whistle-blowers and insider leaks reported in the press), as well as analysis of more than 200 known incidents between 2019-2021. It also offers intelligence from a survey of over 50 leading practitioners in relevant fields, such as cybersecurity, intelligence, government, academia and law enforcement and draws upon informants across the dark net and other covert sources conducted as part of phase II of the Web of Profit research. For further details on methodology please refer to appendix I.

OUR ANALYSIS SHOWS THAT:

01 **Proliferations in cyber-based Nation State struggle mean we may be closer to 'advanced cyberconflict' (ACC) than at any point since the inception of the internet.** Whether it is the frequency of cyberattacks, the phenomenon of hybridisation (i.e. the growing fusion between cyber and physical/kinetic confrontations), or the role of pre-existing regional conflicts in exacerbating and promoting cyberconflict, the writing on the wall is increasingly hard to ignore.

02 **Nations are now prepared to devote significant time and resources towards achieving strategic advantages in cyberspace.**[1] With spending on cybersecurity projected to rise by 11% in the US (between 2019-2021[2]), by 25% in China (to 2023[3]), by 50% in the EU (to 2023[4]) and by up to 200% in Russia (to 2023[5]), the increasing strategic interest of Nation States in cyberspace is clear enough. And with dedicated research programmes aimed at developing new kinds of cyberattacks, the stockpiling of 'exploits', or the combining of attack tools and techniques[6] – there has been a significant complexification in the methods used by Nation States to further these strategic objectives. The wholesale penetration of US cybersecurity at the end of 2020 by way of the SolarWinds hack counts as perhaps the most spectacular and notorious recent example. Yet despite its success, this was only one incident within a much wider field of engagements.

03 **The Web of Profit – i.e. the interconnected, underground cybercrime economies that exist across the world – is shaping the character of Nation State conflict within online environments.** Not only are many Nation States making active use of tools and techniques available within the Web of Profit, some are recruiting cybercriminals to act as proxies to further their interests. Conversely, many tools originating from national security agencies are finding their way into the hands of cybercriminals – an infamous example being the NSA EternalBlue exploit, which was used by the WannaCry hackers in 2017 to cause mayhem worldwide. In this way, Nation States have become both beneficiaries ***of*** and contributors ***to*** the Web of Profit that constitutes the cybercrime economy.

> *"And with dedicated research programmes aimed at developing new kinds of cyberattacks, the stockpiling of 'exploits', or the combining of attack tools and techniques – there has been a significant complexification in the methods used by Nation States to further these strategic objectives.*

1 In military parlance, this augments the four traditional theatres of conflict; land, sea, air and space

2 Slye (2020)

3 Xinhua (2019)

4 Townsend (2019) – this refers to the rise in EU Cybersecurity Agency's (ENISA) budget – from €11 million to €23 million over this period. But the EU is also committed to spending a further €2bn to boost its cybersecurity industry, financing state-of-the-art cybersecurity equipment and similar goals

5 Isvestia (2020)

6 The use of a phishing email (technique) combined with malware (tool) seen in the Sunburst/SolarWinds attack would count as an example here

This unprecedented fusion between politics, strategic manoeuvre, commerce and crime is beginning to pose unique challenges...

This lack of effective regulation, or any sign of consensus on the part of Nation States in trying to develop acceptable standards of conduct online, is not good news.

04 **Nation States are also more prepared to exploit new opportunities.** Their response to the Covid-19 pandemic over the past 12 months presents us with a classic case study of this readiness. On the one hand, the pandemic has overshadowed and overtaken world events significantly during the course of this research, bringing disruption and disorder to many traditional areas of Nation State activity – such as travel and trade. But far from interrupting the developments in Nation State cyberconflict, it has exacerbated them. Whether it is in the struggle to obtain intellectual property on vaccines, or attempts to disrupt supply chains, the Covid-19 crisis has demonstrated the lengths Nation States are prepared to go in using cyber tools to reinforce strategic goals. It has also thrown further light on the entanglements between cybercrime techniques and Nation State cyberattacks noted above, as some of the methods which Nation States have been using to acquire Covid-19 related IP data appear to have been initially road-tested by cybercriminals in their pursuit of more overtly material gain.

The result of the trends highlighted in these findings is something entirely novel; a merging of traditional international relations with the cybercrime economy and the tools and techniques which now drive the digital underground. This unprecedented fusion between politics, strategic manoeuvre, commerce and crime is beginning to pose unique challenges in how to regulate the digital world, especially the search for common areas of interest which can lessen tensions between Nation States.

This lack of effective regulation, or any sign of consensus on the part of Nation States in trying to develop acceptable standards of conduct online, is not good news. Indeed, it serves as a further indication that we may be at far greater risk from the internet than was ever suspected. Accordingly, the report concludes by highlighting findings around the most up-to-date options for cyber-détente. The seemingly diminishing prospects for cyberpeace discussed here further emphasize the challenges for Nation States in preserving their interests within cyberspace, whilst also avoiding conflict escalation. A range of recommendations are provided, including: more active engagement by policy makers in the pursuit of cyber-treaties and cyber-agreements; more involvement from cybersecurity professionals in developing intelligence around typical Nation State cyberweapons and ways of combating them; and better co-operation by enterprise in sharing ways to manage Nation State threats to their data and network capacity.

By deploying new kinds of analysis of the incomplete data we do possess, coupled with expert knowledge to fill in the gaps, we suggest that what follows offers a new basis for developing more informed, better directed responses to the Nation State threat.

KEY FINDINGS: ESCALATION, INTENSIFICATION & EXPANSION

ESCALATION

1 Frequency & Prevalence

100% rise in 'significant' Nation State incidents between 2017-2020[7]

Average of over **10 publicly attributed cyberattacks a month** in 2020

64% of our experts[8] believe 2020 presented a **'worrying'** or **'very worrying'** escalation in tensions within cyberspace

2 Cyber/physical hybridisations

Over 40% cyberattacks had physical and digital component

20% correlated to regional conflicts[9]

INTENSIFICATION

Most common weapons:

78%
rise in supply chain attacks in 2019[10]

37%
of experts say supply chain attacks are one of the 'most significant' methods being developed by Nation States

40%
of security breaches are now indirect[11]

There were **27 known Nation State** supply chain attacks between 2017-2020[12]

Known Nation State targets:

- Enterprise 35%
- Cyberdefence[13] 25%
- Media and communication 14%
- Government bodies or regulatory agencies 12%
- Critical infrastructures[14] 10%

7 CSIS (2020) offers a similar tally
8 Findings from expert panel mentioned in executive summary and methodology
9 Brown (2020)
10 Symantec (2019)
11 Accenture (2020)
12 Herr et al (2020)
13 Cyberdefence is defined as the collective agencies, services, hardware and software with responsibilities for protecting national cybersecurity. This may include agencies like the UK NCSC (National Cyber Security Centre), the US CISA (Cybersecurity and Infrastructure Agency), national CERTs (Computer emergency response teams), intelligence gathering bodies like GCHQ or the NSA, private sector Internet service providers (ISPs), software blocking government users access to suspect sites like the Protective Domain name System (DNS), government firewalls, take down services and so on
14 Other data (O'Malley, 2020), showing that 36% of companies in North America reported Nation State threats between 2019-2020 corroborates this finding

EXPANSION I

the cybercrime economy

20% of cyberattacks involved sophisticated weapons

50% involved low budget tools

65% of experts believe Nation States make money from cybercrime

58% say it's more common for Nation States to recruit cybercriminals

EXPANSION II

Covid-19

75% of experts say Covid-19 represented a 'significant new opportunity' for Nation States to exploit.

40% rise in Nation State incidents between July–September 2020, compared to January–June 2020

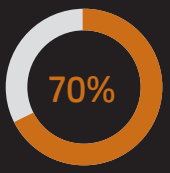
50% rise in cyberattacks on pharmaceutical companies[15]

50,000+ new Covid-19 related sites created between February–May 2020 involved fraud[16]

45% rise in cyberattacks against healthcare organisations since November 2020[17]

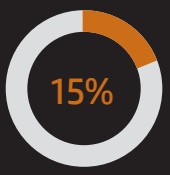
CYBERWAR OR CYBERPEACE?

Will there ever be a cyber-treaty?

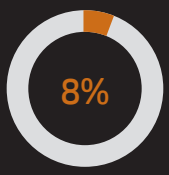


say a cyber-treaty is necessary to prevent escalations in cyberwar

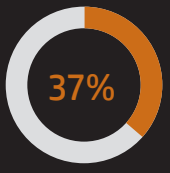
say it'll take over 20 years



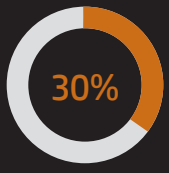
say an agreement will come in the next 5-10 years



said they don't know



say it'll take 10-20 years



believe there is no prospect of any cyber-treaty within any timeframe

15 Coker (2020)
16 Chandler (2020), Lancaster (2020)
17 Lancaster (2020b)

1.1

COMPETITION, CONFLICT, OR ADVANCED CYBERCONFLICT ('CYBERWAR')?

To provide one of the first, more precise assessments of how competition between Nation States should be interpreted in terms of its level of escalation, the research developed a special analytic tool to provide a more definitive mapping of current tensions. The gauge utilises three distinct co-ordinate points:

(i) ***Cyber-competition:*** Where nations use cyberspace aggressively to achieve advantages over competitors, much like economic actors do, though with fewer recognised norms of conduct or limitations upon them. For example, attempts to dominate the domain name system.

(ii) ***Cyberconflict:*** Where nations engage in more aggressive forms of online competition, with strategic objectives beginning to take precedence over economic advantage. Agreement and consensus are devalued, but without turning into overt strife. For example, attempts to probe competitor networks in order to obtain intelligence or other strategically useful data.

(iii) ***Advanced Cyberconflict (ACC):*** Where nations begin to engage in repeated digital attacks and counterattacks. For example, sophisticated cyberattacks aimed at compromising networks and causing loss of functionality. Blurring between on/offline targets, and increased focus upon physical assets, like power grids or water supplies. Potential use of conventional weapons to retaliate against cyberattacks.

We then identified a range of typical indicators of the traditional path to advanced (kinetic) conflicts considered within previous research and adapted these to the digital context[18]. Indicators include: ***evidence of active attempts to increase the number and sophistication of cyberweapons***, and ***evidence that nations seek territorial gain from a war***. By correlating these indicators with parallels within the cyberworld and evaluating the extent to which these held at three timeframes over the past 20 years (2000, 2010 & 2020), it was possible to quantify more precisely how serious the unfolding situation might now be.

18 See, for example, Jackson and Morelli (2009) and Hegre et al (2011)

ADVANCED CYBERCONFLICT HEAT GAUGE

TRADITIONAL INDICATORS OF PATH TO ADVANCED CONFLICT/WAR	CYBER PARALLEL AND EXAMPLES	2000	2010	2020
The perception that there are minimal reasons not to engage in war	Standard cybersecurity tools increasingly fail to prevent targeted Nation State cyberattacks; retaliations to cyberattacks so far limited and largely restricted to upon rival information systems			
The perception that actions by competitors constitute acts of war	The UK attorney general has stated that western powers will regard network incursions as 'a cause for war'[19]			
A sense that gains from war will exceed potential costs	No sanctions for increasing cyber-aggression have been developed since the post 2009 rise in tensions			
Evidence that nations expect economic gain from a war	Many Nation States pursue cyberconflict for revenue generation or other economic benefits			
Retaliations against perceived slights	Increasing evidence of a readiness to respond to any aggressive network incursions			
Failure to communicate or to agree to norms of conduct amongst competitors	An absence of any international agreement around cyberweapons			
A 'youth bulge' (increase in population available for deployment in war)	Increases in young, information technology proficient populations available for deployment by Nation States			
Evidence that nations seek territorial gain from a war	Seeking to 'occupy' or annex rival networks/ digital assets (for example using planted malware hidden for long periods) has become common			
Evidence of active attempts to increase number and sophistication of weapons	Estimated number of cyber-weapons has increased by a factor in excess of 10,000% between 2000-2020[20]			
Religious/ideological disagreement	No obvious parallel, other than cyber aggression provoking magnifications of existing disagreements			
Grievances arising from a previous history of conflict	Frequent translation of offline grievances into cyberspace			

19 Hall (2018)

20 Figure based upon evaluations of known malware types in 2000 and potential uses by Nation States, compared to 2020

Where fewer than four indicators were in place, our expert panel evaluated the situation as nothing more than a form of aggressive *cyber-competition*. Where between four to eight indicators were in place, they evaluated this as a more developed kind of competition which corresponded to a *cyberconflict*. Where more than eight indicators were in place, they judged that conflict was close to, or had already become, an *advanced cyberconflict* (ACC) or, more colloquially, a cyberwar.

This kind of measure is useful in highlighting the clear rise in tensions over the last 20 years. In 2000, fewer than four indicators were unambiguously in place, so Nation State relations in cyberspace was still largely about gaining competitive advantage. By 2010, around seven indicators were arguably in place, indicating an increasing slide into more overtly conflict-based relations. In 2020, with at least 11 factors now in place, current prognoses are concerning. With the cumulative growth of indicators, such as increased weaponisation and the readiness of government representatives to define hostile network incursions as 'acts of war'[21], we have moved to a dangerous stage. Equally, if not more concerning, is the lack of public awareness about the potential gravity of these increasing tensions.

2.1

NATION STATES IN CYBERSPACE: THE CHARACTERISTICS OF NATION STATE CYBERCONFLICT

Given that Nation States now use digital networks to aggressively compete for influence in ways which often stand outside usual norms of conduct, it has become increasingly important to be able to identify and characterise these strategic dynamics. At least 10 distinctive features of Nation State cyberconflict were identified in this research:

(i) **Asymmetric.** Smaller powers can successfully confront larger powers.
   a. Over **70%** of the incidents analysed for this research involved Nation States under attack by, or in conflict with, groups of less than 15-20 individuals.

(ii) **Invisible.** Cyber-armies rarely march in formation or behind flags to indicate their loyalty.
   a. The 100% denial rate is underscored by the fact that, to date, no state has confessed to any cyberattack, even where evidence is clear.

(iii) **Molecular.** Struggles may involve multiple agents, often in combination.
   a. For example (potentially several) Nation States; any proxies or mercenaries they use; intelligence agencies engaged in subterfuge; cybersecurity firms responding to or inviting cyberattacks (as with a honeypot) and even cybercrime groups.

(iv) **Multi-dimensional.** Cyberconflict increasingly involves cyberattacks which extend beyond rivals' information systems/cyberdefences into their physical assets.
   a. Over **40%** of the incidents analysed in the research involved an attack upon assets which had a physical and digital component.

(v) **Glocal'**[22]. Cyberconflict manifests significant interdependences between regional and global struggles, with the former often a springboard for the latter.
   a. Around **20%** of the incidents we analysed had their origins in regional cyberconflict.

21 Assertions of this kind have recently been made by the British Attorney General (Hall, 2018) and the EU (Muncaster, 2017). Similarly, the US has declared that attempts to compromise networks could, in certain circumstances, "constitute an armed attack" (Wolfe, 2019)

22 This term originates in Robertson (1994)

(vi) **Personal.** Nation States have been increasingly ready to directly target individuals considered to pose a threat in the pursuit of their strategic cyber interests.
   a. Recent examples include: the 2018 hack and release of compromising photographs of Amazon CEO, Jeff Bezos, by a Nation State actor,[23] and widespread digital surveillance of individuals considered to pose a threat to Nation States[24].

(vii) **Prismatic.** Cyberconflict increasingly acts as a reflection of other kinds of extra-military conflicts – such as trade wars – whilst simultaneously amplifying reciprocal tensions.

(viii) **Hybridised.** Cyber operations are increasingly conducted in conjunction with or as response to physical conflict.

(ix) **Agnostic.** It can often be difficult to separate friends from foes within cyberconflict.
   a. For example, details released in 2013 by the CIA whistle-blower Edward Snowden revealed how the NSA had been tapping the phone and communications of the German Chancellor, Angela Merkel, along with senior EU officials, 35 other world leaders, and more than 70 million French citizens[25].

(x) **Cultural.** Whether it is the influencing of elections, or the 'cognitive hacking' of attitudes on social media, cyberconflict has a far more subversive impact upon the socio-cultural fabric of enemy societies than traditional war.
   a. For example, a body of research now indicates that false stories placed in social media tend to be liked and shared far more than true stories, have a longer shelf-life and a far wider spread of distribution[26].

23 Merriman (2019)
24 Ignatius (2018)
25 Ball (2013)
26 See, for example, Silverman (2016)

2.2

STRATEGIES, OBJECTIVES, TARGETS & TOOLS

Identifying individual cyberattacks is one thing, but a more complete understanding of Nation States' approach to cyberconflict requires filling the gaps in data to discern key patterns and dynamics.

For this research, we developed the **NSiC** (Nation States in Cyberspace) method of analysis. An NSiC approach uses a process of synthesis and simplification to make the many complex decisions and motivations which drive Nation State cyberattacks within cyberspace more immediately transparent to analysts. To achieve this, four key **'SOTTT'** variables are used to map Nation State conduct:

In this way the NSiC provides a more integrated picture of incidents, enabling clearer breakdown and comparison. In addition, it facilitates a more joined up, holistic understanding of the way typical cyberconflicts develop and are maintained. Each of the four variables are broken down as follows:

STRATEGY

Whilst closely connected, a key difference between cybercrime and Nation State activity involves the ***strategy*** being pursued – that is, the overall, long-term plans and actions aimed at acquiring advantages. Better understanding of a strategy can tell us a great deal about why Nation States are using cyber tools in certain ways and so help foster more informed responses. By analysing a range of offensive actions by Nation States drawn from our incident database, we identified 14 distinct strategies Nation States appear to be using to gain advantages from cyberconflict. Though the list is clearly a simplification (Nation States will operate in other ways and in more than one way on occasions), it serves as a useful thumbnail guide for understanding how (and why) Nation States may favour certain strategic options over others.

> *Better understanding of a strategy can tell us a great deal about why Nation States are using cyber tools in certain ways and so help foster more informed responses.*

STRATEGY	CHARACTERISATION
Domination	Advantage gained by full spectrum control over cyberspace
Accumulation	Advantage gained by building assets such as currency or data
Penetration	Advantage gained by breaching digital, physical or cognitive protections
Retaliation	Advantage gained by reminding enemy that aggressive action always has a reaction
Absorption	Advantage gained by emulating or taking over techniques and assets
Facilitation	Advantage gained by enabling other Nation States
Protection	Advantage gained by preserving/reinforcing digital, physical or political structures
Extraction	Advantage gained by illicit acquisition of rival's assets like data
Disruption	Advantage gained by bringing disorder into an enemy's defences
Negotiation	Advantage gained by forging consensus
Elimination	Advantage gained by permanent removal of threats – real or perceived
Reinforcement	Advantage gained by enhancing existing resources of structures
Infiltration	Advantage gained by covertly accessing rival's systems
Demonstration	Advantage gained by making a show of strength or capacity

Figure 1 – Typical Nation State strategies employed in cyberspace

For example, strategies such as *Domination* enable a state to gain advantage by explicit attempts to take control over cyberspace whilst *Extraction* enables an advantage by illicit acquisition of rival's digital assets.

OBJECTIVE

Nation States often pursue more immediate objectives in addition to their longer term strategies. Effective, more nuanced analysis therefore requires a combination of objective with strategy. Four typical objectives which shape the conduct of Nation States in cyberspace were derived from analysis of our incident database, correlated with survey data obtained for this research. These are detailed in the table below:

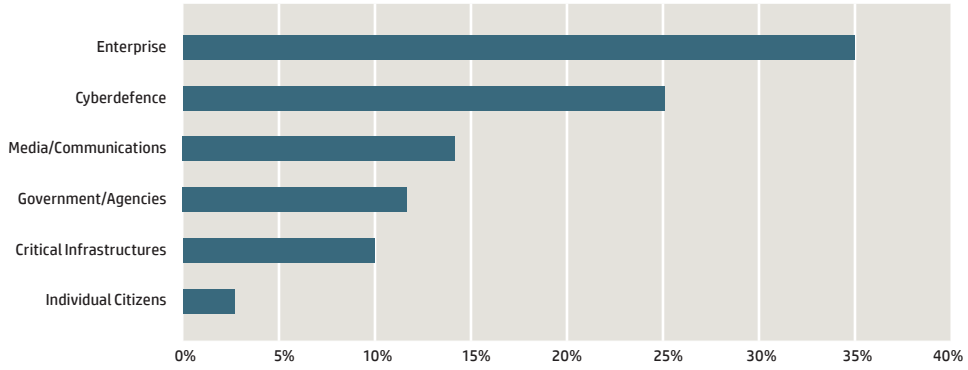
OBJECTIVE	SUB-PURPOSE	EXAMPLE
Acquisition	Intelligence	Acquisition of military, industrial or political secrets/intelligence. For example, around 95% of cyberattacks in the manufacturing sector are now associated with acquisitional espionage.[27]
	Data	Around 20-25% of data breaches in 2018/19 are likely to have involved Nation State actors[28].
	Revenues	Some Nation States may now be generating revenues equivalent to 30% of their export revenues from cyberattacks (see appendix II).
	Status	Symbolic cyberattacks which indicate capacity, like the 2014 Sony pictures hack[29].
Incapacitation	Sabotage	Damage or incapacitation of enemy assets – e.g. the Shamoon cyberattacks on Gulf Oil companies using the Disttrack malware which wiped files and rendered systems inoperative[30].
	Disruption	Impairing network functionality. Internet shutdowns or network disruptions have been estimated to cost Nation States around $2.4 billion annually[31].
Shaping	Opinion	'Cognitive hacking' – such as disseminating disinformation to spread social conflict or division. For example, the increasing use of 'Twitter bots' by Nation States to promote extremist views, or to disrupt electoral processes[32].
	Regime change	Amongst the many examples here are interventions by rival Nation States in Ukraine against the nationalist government; interventions in Venezuela, including possible cyberattacks on critical infrastructure such as lighting[33].
Hybridisation	Tactical support	Use of cyber capacity to augment success of conventional forces – e.g. the 2019 US cyberattacks on Iranian missile capacity[34].

Table 1: Nation State objectives in cyberconflict[35]

27 SOFF (2017)
28 Verizon (2019)
29 Elkind (2015)
30 ENISA (2019)
31 West (2016)
32 Guglielmi (2020)
33 Leetaru (2019)
34 Lewis & Unal (2019)
35 Note that these do not need to be mutually exclusive. A Nation State may have the objects of obtaining data which serves in secondary objectives such as intelligence and revenue generation

TARGET

Strategy and objective are linked by a third factor crucial to understanding Nation State conduct in cyberspace – the ***targets*** of typical cyberattacks. By correlating analysis of our incident database with other research in the field[36], some of the most commonly targeted assets were identified as the following.



Graph 1: The most common targets of Nation State cyberattacks

> *The most frequent target for Nation State cyberattacks (representing 35% of cyberattacks analysed) is business and enterprise.*

Enterprise – The most frequent target for Nation State cyberattacks (representing **35% of cyberattacks analysed**) is business and enterprise. Irrespective of sector or size, business appears now to face comparable risks from Nation States as it has done from traditional cybercriminals. Obtaining IP or business intelligence has provided one obvious motivation, with technology firms and pharmaceutical/biotech firms at particular risk. Data from 2020/21 suggests that the Covid-19 pandemic has exacerbated this trend. For example, attempts to acquire intellectual property related to the Covid-19 virus (such as information about vaccine development) has been associated with a reported rise of around **50%** in hacking and ransomware attacks on pharmaceutical companies like Pfizer[37]. This has also been paralleled by espionage against research labs and disruptions to healthcare, with a rise of **45%** in cyberattacks against research labs and hospitals treating Covid-19 patients since November 2020[38]. Nation States can be clearly associated with such activity, with around **38%** of malicious actors involved in cyberespionage attributed to Nation States between 2019-2020[39].

> *...attempts to acquire intellectual property related to the Covid-19 virus (such as information about vaccine development) has been associated with a reported rise of around 50% in hacking and ransomware attacks on pharmaceutical companies like Pfizer.*

No enterprise appears to be safe from the threat of Nation State cyberattacks. For example, the APT10 group (aka ***Menupass*** or ***Red Apollo***)[40] which has specialised in IP theft, has also been associated with hacking into US law firms in order to obtain data on clients in key industries[41]. APT10 has also targeted the IT industry, large clothing companies, aerospace and heavy industry.[42] Small businesses appears to be equally at risk – as highlighted in cyberattacks during 2017/18 conducted by the APT28 group (aka ***Fancy Bear***, ***Sofacy*** or ***Pawn Storm***). Thousands of small business and home-based routers were hacked and placed under the group's control[43]. APT28, which was previously associated with the hack into the US Democratic Party during the 2016 election, has recently begun to probe vulnerable email servers across the enterprise and other sectors – probably to acquire credentials and to extract useful data from emails[44]. APT28 have also explored a growing trend in acquiring access to corporate networks through the use of IoT devices such as office printers and video decoders. Evidence emerged in 2019 of attempts by the group to use such devices, together with VoIP phones, to compromise other vulnerable machines on the network. In this way, access to more restricted accounts with more

> *APT28 have also explored a growing trend in acquiring access to corporate networks through the use of IoT devices such as office printers and video decoders.*

36 See, for example, CrowdStrike (2019) and FireEye (2019)
37 Coker (2020)
38 Lancaster (2020b)
39 ENISA (2020)
40 Please note that APT groups are often referred to by a variety of different names, and not always consistently across different sources. This report has adopted the convention of ***number designation***, followed by two - three of the most common names associated with the group
41 Leyden (2019)
42 NSCS (2018b)
43 Lucero (2018)
44 Muncaster (2020)

New malware strains like the Kaji variety, which uses simple SSH brute-force/dictionary attacks to take over IoT devices further emphasize why effective endpoint security and continuous testing are now essential tools to protect corporate networks against Nation State threats.

The next most frequent target we found was national cyberdefence (25% of cyberattacks), whilst cyberttacks upon specific government and regulatory bodies made up around 12% of those incidents.

Potentially more deadly threats come from the emergence of firmware attacks such as Lojax, which is able to situate itself at the deepest operating level – the so-called 'Unified Extensible Firmware Interface (UEFI) which deals with booting and loading the operating system.

valuable data could be attained[45]. New malware strains like the Kaji variety, which uses simple SSH brute-force/dictionary cyberattacks to take over IoT devices[46] further emphasize why effective endpoint security and continuous testing are now essential tools to protect corporate networks against Nation State threats.

Other cyberattacks upon enterprise email vulnerabilities emerged in 2021 when the Hafnium Advanced Persistent Threat (APT) group deployed various zero-day exploits to target the Microsoft Exchange server. They were able to compromise emails, steal data and plant malware which enabled remote access over extended periods. Over 20,000 organisations were targeted including enterprises such as banks, financial institutions, electricity companies, as well as small hotels, and other mid-market businesses[47].

One of the most recent examples of the vulnerability of enterprise to Nation State cyberattacks occurred in 2020 when the Orion software, used by the SolarWinds company was targeted. This was then used in a supply chain attack to obtain legitimate credentials permitting undetected access to the systems of significant numbers of leading US companies. Over **15,000** SolarWinds clients had their networks compromised, including many of SolarWinds' Fortune 500 enterprise clients, especially within the IT sector, including Cisco, FireEye, Intel and Microsoft[48].

Cyberdefence & Cyberattacks Upon Government Agencies[49] – The next most frequent target we found was national cyberdefence (**25%** of cyberattacks), whilst attacks upon specific government and regulatory bodies made up around **12%** of incidents. Clearly Nation States regularly need to deal with cyberattacks upon their cybersecurity/cyberdefence systems whether these are to probe strength, to disrupt operations or to extract useful data. As a result, testing cybersecurity can often be combined with more direct attacks upon government agencies. For example, the 2018 'Synthetic Theology' operation conducted by US Cyber Command to probe other countries' networks for threat intelligence[50]. There has also been an increasing interest in targeting the broader internet infrastructure itself. In 2019 for example, there were two distinct examples of such cyberattacks. One was aimed at the Domain Name (DNS) structure enabling snooping and redirection of traffic, etc. A second involved attacks upon mobile networks to acquire all call log data. Potentially more deadly threats come from the emergence of firmware attacks such as Lojax, which is able to situate itself at the deepest operating level – the so-called 'Unified Extensible Firmware Interface' (UEFI) which deals with booting and loading the operating system[51]. This means that the malware can't be removed by reinstallation or even by wiping the hard drive. Though examples have been rare to date and have been largely associated with cyberespionage attacks targeting diplomats and NGOs, it is clear that firmware carries significant potential as a more all-purpose cyberweapon.

Understanding or disrupting the operations of rival governments has been a special focus of some APT adversaries, such as the Turla group. Turla has been associated with attempts to hack the Chemical Weapons agency in the Hague, and the UK Defence and Science Technology Laboratory (DSTL) computer systems in 2018[52]. In 2020, it was linked to a (successful) ransomware attack on 20 leading universities in the UK, US and Canada – just one example of an emerging attack vector, with an average of around a thousand cyberattacks per year on UK universities alone between 2018-2020[53]. The 2020 Sunburst supply chain attack also involved penetrations to key government agencies like the US Department of Homeland Security; US Department of State; US National Institutes of Health; US Department of Commerce and the US Department of the Treasury.

Media & Communications– Acquiring access to rival Nation States' media and communication systems has been an increasingly attractive option, constituting around **14%** of Nation State cyberattacks. Influencing agendas, degrading the quality of information available to a rival public, or straightforward

45 Vavra (2019)
46 Daws (2020)
47 Seal (2021)
48 Krebs (2021)
49 Cyberdefence is defined as both the tools and techniques utilised to protect key networks, infrastructures and other digital assets
50 Nakashima (2019)
51 Higgins (2020)
52 Crerar et al (2018) & Gov. UK (2018)
53 Coughlan (2020)

There are now well over 1,000 attempted hacks on broadcasters every day combined with a still wider targeting of communications systems which now appears to be emerging.

A wave of recent incidents has confirmed these suspicions and our data showed that cyberattacks upon infrastructure now constitute at least 10% of Nation State incidents.

...we should not forget that the inherent asymmetries of force within cyberconflict has meant that strategies of retaliation, infiltration or elimination can sometimes entail direct cyberattacks by Nation States upon individual citizens.

surveillance and intelligence gathering all count as strategic motivations here. The 2015 hack of the French TV5 Monde which resulted in 12 of its channels being taken offline for 18 hours is one notorious example[54]. Attacks by the Sandworm APT upon media company computers in Ukraine is a more recent case[55]. There are now well over 1,000 attempted hacks on broadcasters every day[56] combined with a still wider targeting of communications systems which now appears to be emerging. For example, not only have traditional news sites like the BBC, been spoofed to spread disinformation[57] but newer encrypted messaging tools, like WhatsApp, WeChat or Telegram are being increasingly targeted by Nation States. In 2019, the WhatsApp accounts of senior government and military officials in at least 20 countries allied to the US were hacked[58] and in 2020, Twitter reported that a 'state-sponsored actor' had been able to boost the viral impact of posts by linking phone numbers to Twitter usernames[59]. Obtaining covert communications like diplomatic cables has been another trend. For example, the recent leaking of confidential government messages by the former UK ambassador to the US, very likely by a hostile cyberpower[60].

Critical Infrastructures – Critical infrastructures like power grids or water supply systems, have long figured in the imagination of commentators as potential targets. A wave of recent incidents has confirmed these suspicions and our data showed that cyberattacks upon infrastructure now constitute at least **10%** of Nation State incidents. In a 2019 survey of security staff in the utility, energy, health and transport sectors[61], it emerged that 90% reported at least one successful attack on their installations between 2017-2019. For example, intrusions in 2014 on US energy utilities that were infected with the Black Energy malware[62], appear to have been a dress rehearsal for attacks in 2018 by the Sandworm or Voodoo Bear APT, upon various Ukrainian energy infrastructures using the same malware. The Ukraine railway ticketing system was also compromised by the same group. Cyberattacks on meteorology systems which supply climate information to shipping and airline companies have also been reported[63].

Individual Citizens – Finally, we should not forget that the inherent asymmetries of force within cyberconflict have meant that strategies of retaliation, infiltration or elimination can sometimes entail direct cyberattacks by Nation States upon individual citizens. Such attacks may be fewer in volume (< 5% of the sample we analysed) but may have important long-term consequences. Whilst assassinations of private individuals or attacks upon their reputation have long been practiced by Nation States, the advent of digital networks has provided new options, often conducted in conjunction with on the ground activity. Definitive evidence is limited, but there are certain well documented incidents of this kind. For example, tweets infected with malware were sent in 2017 to US Defence Department employees and family members using Twitter. The messages appear to have been carefully targeted to appeal to individual interests and resulted in click rates of around 70 percent. Home devices with sensitive government information were compromised as a result[64]. Journalists considered to be subversive by certain Nation States have been subject to surveillance[65], whilst high profile individuals have also been targeted. For example, attempts to defame Jeff Bezos, the CEO of Amazon, by circulating (hacked) compromising photos were associated with a hostile Nation State actor[66].

Beyond more prominent targets like the above, we should not overlook other less obvious examples. For example, strategies of **infiltration** where an objective is to disrupt competitor societies, have produced increasing attempts to target socio-cultural processes and institutions, in particular elections[67].

TOOLS & TECHNIQUES

The successful combination of strategy and objective with a target will usually centre upon the successful delivery of a cyberweapon. However, deciding what to count as a cyberweapon has often been less than clear. Cyberweaponry could refer to a tool or a technique. It could refer to a destructive capability – one that damages systems or simply steals data[68], or may involve tools that seek to influence public opinion on social media.

54 Corera (2016)
55 RTS (2016) & Hern (2016)
56 Snoddy (2016)
57 Elliott (2019)
58 Reuters (2019)
59 Doffman (2020)
60 Jones (2018)
61 Simmons (2019)
62 Greenberg (2017)
63 BBC (2015)
64 Bosetta (2018)
65 Ignatius (2018)
66 Kirschgaessner (2020)
67 See, for example, Shane (2018), BBC (2019 & 2019b) & JTA (2019)
68 See, for example, Uren et al (2018)

This ambiguity has seen this research attempt to develop a more general **typology** of cyberweapons, which treats tool and technique as part of their overall character, together with other factors like the context in which they are used. This typology defines cyberweapons in terms of their objective, cyberweapon type, level of sophistication (5 requiring the longest development time and resources for development, 1 requiring the least time and resources), and application.

This table is only ***one*** snapshot example of a cyberweapon matrix (others are possible) and due to the varying nature of Nation State strategies and objectives, it would be misleading to analyse any one weapon in terms of one purpose. Thus, malware or DDoS attacks only become cyberweapons when they are used in certain ways or have been developed to differing degrees of sophistication. The aim of the matrix then, is to allow us to think of cyberweapons more holistically using a combination of factors.

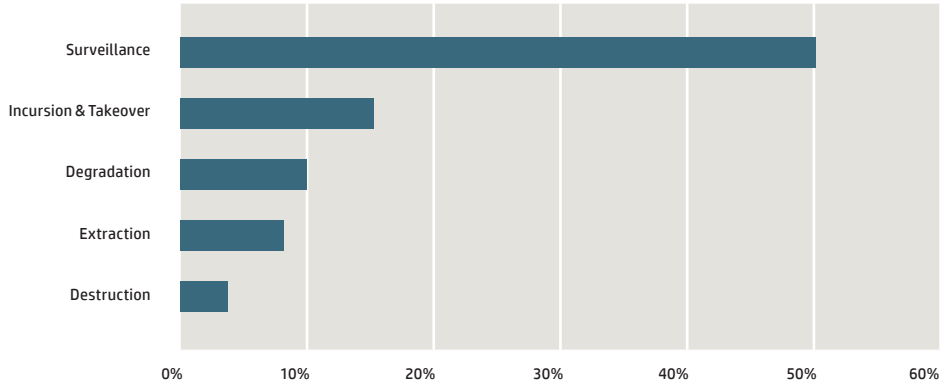
OBJECTIVE	CYBERWEAPON	SOPHISTICATION	APPLICATION
Acquisition			
Intelligence	Hardware backdoors	4	'Lojax' malware which acts like a rootkit, but attacks UEFI – the fundamental key to any computer. Can even survive reinstallations of operating systems and has been associated with cyberespionage operations[69].
Intelligence	RAT (remote access Trojan)	3	2019 use of PlugX RAT by the APT10 group in cyberattacks against SE Asian government and private sector organisations.[70]
Data	Keyloggers	3	QWERTY keylogging malware – a plug-in for the NSA REGIN cyberweapon[71] with mass surveillance applications.
Revenues	Ransomware	2	SamSam ransomware, linked to Nation State cyberattacks on cities like Atlanta, San Diego. Made over $6m by November 2018[72].
Status	Logic bombs	2	Malware planted on Sony Pictures. More than 4,000 computers wiped when 'detonated' following release of a satirical film about the North Korean leader[73].
Incapacitation			
Disruption	DDoS/Botnet	2	2018 DDoS attack on Github software hosting co. – one of the largest ever. Hit by 1.35 tbps of traffic causing temporary loss of service. Strong suspicions of a Nation State actor given a similar DDoS attack conducted in 2015[74].
Disruption	Wiper Malware	3	The NotPetya malware, which emerged in late 2016 and spread rapidly in 2017 disguised itself as ransomware. In fact, it was an endpoint wiper aimed at causing maximum disruption to systems[75].
Sabotage	Worms and targeted malware	5	The Disttrack worm – sophisticated malware used within the 'Shamoon' cyberattacks to target Gulf oil companies and delete data or disrupt operations.
Disruption	Malware framework (incorporating a range of tools)	4	Triton cyberweapon used to take over safety systems in Saudi petrochemical plants. Attribution to one or more Nation States.[76]

69 Goodin (2019)
70 Stewart (2019)
71 Smith (2015)
72 Hoffman (2019)
73 Elkind (2015)
74 Tannam (2018)
75 Thomson (2017)
76 Sherman & Zoob (2018)

> *...applications for surveillance (around 50% of weapons use) appears to far exceed uses for damage (10%) or overt destruction (4%) at present.*

Table 2: A sample cyberweapon matrix

An advantage in categorising cyberweaponry in terms of a matrix of factors, rather than a single definition, is that it permits many other kinds of cyberweapon to be analysed and compared. For example, the many other potential varieties of cyberweapon not listed here could include exploits, backdoors, Trojans, rootkits, and so on[77]. By analysing incidents in our database and comparing



this with other sources[78], it was possible to define the most common uses of cyberweapons by Nation States.

Graph 2: The most common uses of cyberweapons by Nation States

These findings again emphasise how cyberweaponry rarely adheres to traditional patterns of weapon use. For example, applications for surveillance (around **50%** of weapons use) appear to far exceed uses for damage (**10%**) or overt destruction (**4%**) at present. Similarly, network incursion and takeover uses, such as lateral movement (where attempts are made to broaden and cement a foothold to valuable data or systems[79]) or the use of RATs (remote access Trojans), appear to be more frequent than extraction – i.e. stealing data or assets (around **8%**).

Three further observations which seem potentially significant arise from this analysis:

(i) The growing tendency for 'mediated attacks' which evade the need for more sophisticated cyberweapons. The phenomenon of 'supply chain attacks' which target vulnerabilities in software suppliers in order to penetrate government agencies are amongst the most serious examples. For example, the NotPetya Nation State attack used Ukrainian accounting software to target the country's infrastructure and ended up doing more than $10 billion in damage as it spread more widely, also disrupting operations for multinational corporations such as FedEx, and Merck. In late 2020, the SolarWinds[80] hack discussed earlier became one of the most serious of all supply chain attacks – not just because of the wide range of government agencies that were compromised, but because it is now thought to have been exploited by **two** rather than just one Nation State actor, with "massive" consequences for US security according to

77 DeVore & Lee (2017)
78 See, for example, the network traffic reports in Lightcyber (2016) and the incident database in Maness et al (2017)
79 NCSC (2018)
80 Korolov (2021)
81 Reuters (2021)
82 ITRC (2020)

The number of entities affected by supply chain attacks are estimated to have risen by over 100% in the second half of 2020.

...the practice of war and the pursuit of crime have become inextricably interwoven in the contemporary world and cyberweaponry has been central to this blurring of boundaries.

former government officials[81]. The number of entities affected by supply chain attacks are estimated to have risen by over **100%** in the second half of 2020[82].

(ii) How interchangeable cyberweaponry is with tools used in the pursuit of mundane cybercrime. As the report has suggested, the practice of war and the pursuit of crime have become inextricably interwoven in the contemporary world and cyberweaponry has been central to this blurring of boundaries.

(iii) The fact that we are only at the beginning of developing more sophisticated, customised cyberweaponry. Not only are further refinements to existing tools likely, there is a 'second generation' of cyberweaponry on the way that is likely to decisively influence the outcome of future cyberwars. These newer weapons will draw upon enhanced capacities in computing power, more advanced AI, or more complete cyber/physical integration. Five examples are presented below:

2ND GENERATION CYBERWEAPON	POTENTIAL STRATEGIC APPLICATIONS
'Boomerang' Malware	'Captured' malware which can be turned back to operate against its owners. There is evidence that China has already been successful in this[83].
Weaponised Chatbots	AI devices with enhanced capacities to: deliver more persuasive phishing messages; quickly react to new events and send message responses via social media like Twitter; attack other bots[84].
Deep Fakes in Cyberphysical War	Alterations to digital battlefield data (e.g. faces, voices) distorting what is occurring on the ground[85].
Drone Swarms	Drones capable of hacking, disrupting communications like Wi-Fi and Bluetooth, or engaging in surveillance[86].
Quantum Computing	Devices with exponential (quantum based) computing power, able to break almost any encrypted system[87]. China is known to be engaged in extensive research in this area and may have already outstripped Western expertise[88].

Table 3: New directions in cyberweaponry

83 Cushing (2019)
84 Wall (2018)
85 South (2018)
86 O'Neill (2018)
87 Walden & Kashefi (2019). See also Katwala (2018)
88 Katwala (2018)

2.3

NATION STATES IN CYBERSPACE – ANATOMY OF A NATION STATE CYBERATTACK

...unambiguous victory is rarely the aim of cyberconflict – which means that military strategies designed around 'battlespace supremacy' (whether land, sea or air) become irrelevant.

The kinds of factors identified in the NSiC help illustrate why cyberconflict is so different from traditional kinetic conflicts. The purpose of conventional war has usually been to achieve victory, or at least to degrade the enemy sufficiently for the 'victor' to impose their will. But unambiguous victory is rarely the aim of cyberconflict – which means that military strategies designed around 'battlespace supremacy' (whether land, sea or air) become irrelevant.

For example, as the below figure suggests, cyberattacks are rarely one-off incidents, usually consisting of at least four stages, from a planning and pre-attack stage, through to the attack itself and its follow-ups.

PLANNING	PRE-ATTACK	ATTACK	FOLLOW-UP
Development of capacity (training, investment, R&D etc.)	Dry runs	Application of specific attack vector (social engineering, drive by, etc.)	Further continued probing of detected weaknesses
Selection of targets	Practice hacks	Delivery of payload	Ongoing activation of assets in place
Evaluation of weaknesses	Target softening		Follow-up attacks
Weaponisation of key tools	Refining skills		Further weaponisation
	Testing weaknesses		
	Degrading defences in advance		

Figure 2: The stages of a typical Nation State cyberattack

3.1

EXPANSION – NATION STATES AND THE WEB OF PROFIT

One of the most striking findings of this research has been the unprecedented way in which Nation State cyberconflict appears to have become interwoven with many of the activities more typical of the (illicit) digital economy defined as the Web of Profit.

One of the most striking findings of this research has been the unprecedented way in which Nation State cyberconflict appears to have become interwoven with many of the activities more typical of the (illicit) digital economy defined as the Web of Profit. In parallel with this has been the reciprocal cross-over between tools and techniques used by cybercriminals and those used by Nation States.

At least four dimensions to this shift were identified in the research:

(i) **Adoption of Cybercrime Techniques**: Approaches originally refined by hackers and eventually cybercriminals (such as SQL cyberattacks, the use of DDoS, or attempts to spread infection) have been widely adopted by Nation States as strategic options.

For example, there has been an increase of over **200%** in DDoS attacks against international agencies such as the IMF, the UN, and the US State Department recorded between 2017-2018[89]. The motivations for such cyberattacks do not appear to be explicable in terms of traditional cybercriminality.

The expertise manifested in many cyberattacks suggest that not only are Nation States directly employing cybercriminals as proxies, but their resources are allowing them to enhance criminal skills in many cases.

89 D'mello (2019)

Traditional protections against well directed Nation State cyberattacks do not appear to be very effective, with well tested ways to bypass at least 39% of all antivirus tools.

...around 50% involved low budget, straightforward tools easily purchased on the dark net, or other cybercrime markets; around 20% involved more sophisticated custom-made weapons, such as targeted malware or weaponised exploits, probably developed within dedicated state cybersecurity programmes.

...10–15% of dark net vendor sales now go to 'atypical' purchasers or those acting on behalf of other clients.

...data stolen from multiple US government agencies during the SolarWinds hack has been reputedly advertised for sale on the dark net for over $1 million.

For example, Nation State cyberattacks appear to be far more efficient than those enacted by cybercriminals – taking, on average, only 20 minutes to crack most networks[90]. They are also much harder to stop. Traditional protections against well directed Nation State cyberattacks do not appear to be very effective, with well tested ways to bypass at least 39% of all antivirus tools[91].

(ii) **Integration of Cybercrime Tools**: Tools standardly used by cybercriminals (such as malware, keylogging and surveillance devices) are being acquired and weaponised by Nation States.

For example, the sample of cyberattacks between 2010-2020 that were analysed for this research suggest that around **50%** involved low budget, straightforward tools easily purchased on the dark net, or other cybercrime markets; around **20%** involved more sophisticated custom-made weapons, such as targeted malware or weaponised exploits, probably developed within dedicated state cybersecurity programmes. A further **30%** were of uncertain, or unattributable origin.

The trade in unmonitored, off-the-shelf cyberweapons, acquired by Nation States through the dark net or more covert sources, may be significant – though this is impossible to establish definitively. According to a sample of dark net vendors interviewed for this research and as part of the previous report on dark net cyber threats, anything between **10–15%** of their sales now go to 'atypical' purchasers or those acting on behalf of other clients[92]. Some of these involve the phenomenon of 'stock-piling' tools like zero-day exploits[93].

It is also clear that many dark net markets now operate along Nation State lines with listings in the language of the state in question, and products customised to the specific needs of domestic producers and consumers[94].

(iii) **Nation State Digital Resources Being Traded and Used by Cybercriminals**: A converse flow of digital resources has begun to flow in the opposite direction, with the result that cybercriminal activity often now benefits from sophisticated hacking tools originally developed by Nation States or from data generated by government agencies. There are even cases of governments actively sharing hacking tools. For example, the penetration testing tool PowerShell Empire has proved such a favourite for hackers that it was identified as one of the five most dangerous public hacking tools by the UK National Cyber Security Centre[95]. But it also has been widely used by Nation State sponsored APT groups to compromise cloud services, extending its spread via Covid-19 phishing emails in 2020[96].

Elsewhere, EternalBlue, one of the exploits acquired from the US National Security Agency (NSA) in the notorious Shadow Brokers leak has now helped compromise over five million computers worldwide. It has caused several billion dollars of losses to businesses and governments globally and generated in excess of $500 million in revenues for cybercriminals[97].

More recently, data stolen from multiple US government agencies during the SolarWinds hack has been reputedly advertised for sale on the dark net for over $1 million[98].

(iv) **Nation States Profit from the Cybercrime Economy**: The huge value of an economy based around cybercrime activity has allowed some Nation States to engage with this for direct revenue generation, or for more indirect benefits. For example, through the (illicit) acquisition of digital currencies; data-theft and trading; intellectual property and trade secret theft; or simply the sale of devices, which blur the boundaries between cybersecurity and cyberweaponry. The resulting revenue streams seem to be having increasing impacts upon traditional Nation State economic indicators such as Gross Domestic Product (GDP), foreign currency reserves, or export value.

90 Kundaliya (2019)
91 Ashford (2018)
92 McGuire (2019)
93 cf Maxwell (2017)
94 Osbourne (2016)
95 NCSC (2018)
96 Jay (2020)
97 cf Perloth & Shane (2019)
98 Abrams (2021)

3.2

REVENUE GENERATION AND THE WEB OF PROFIT

Militarisation can certainly influence an economy – as seen in the impact of increases in arms production upon a nation's GDP. Nation State cyberconflict appears to have added a new dimension to this relationship. In previous reports, our research has identified the significant scale of the cybercrime economy which – even on relatively conservative estimates – appears to be generating over **$1.5 trillion** in revenues annually[99]. Given that the scale of this cybercrime economy (as a whole) now not only outstrips the profits made by Fortune 500 companies, but the GDP of many Nation States, obvious temptations are presented for exploiting these revenue flows.

"Given that the scale of this cybercrime economy (as a whole) now not only outstrips the profits made by Fortune 500 companies, but the GDP of many Nation States, obvious temptations are presented for exploiting these revenue flows.

Typical sources of revenue may include:

- trade secret theft or data trading
- theft in currency
- digital money laundering
- the lucrative (albeit legal) industry of building cybersecurity tools

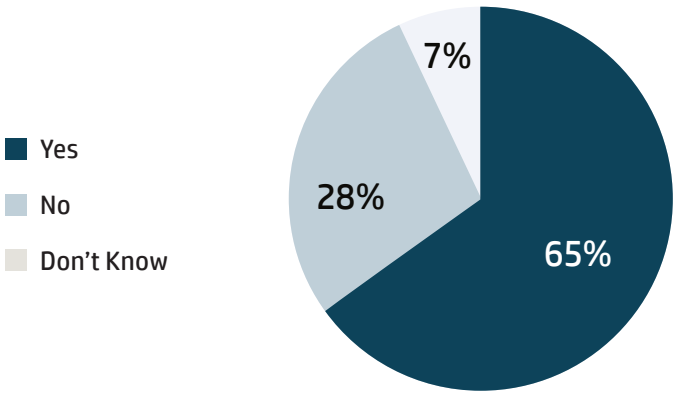
One relatively well evidenced example of exploiting the cybercrime economy has been the case of North Korea (DPRK). Most experts believe that it has been able to combine methods of generating revenues from cybercrime with digital innovation. One approach has been bank robbery; albeit in forms such as cryptocurrency theft, ransomware operations, or money laundering. For example, a well evidenced set of cyberattacks on cryptocurrency exchanges in 2017 generated revenues equivalent to $571 million for the North Korean Lazarus APT group. The group used phishing and other techniques to access the exchange, providing a useful way of supplementing the North Korean government's limited access to foreign currency. Similarly, North Korean groups, probably government sponsored, were involved in a 2016 attack using SWIFT credentials from Bangladeshi Central Bank employees to engineer an $81 million transfer – one of a series of attempted heists from banks in South East Asia by the group[100]. In 2018, the group switched their attention to ATM hacks, successfully engineering them into paying out millions of dollars on command using a specially adapted Trojan[101]. A 2021 report by the UN has suggested that over $300 million generated by the DPRK in 2020 through cybertheft was used to fund its nuclear and ballistic missile programmes[102].

"...almost two thirds (65%) of the respondents to our expert survey believe it is possible for Nation States to make money out of cybercrime..."

The impression of Nation States' direct involvement in cybercrime appears to be becoming more widespread; almost two thirds **(65%)** of the respondents to our expert survey believe it is possible for Nation States to make money out of cybercrime – an opinion that has also been acknowledged by the major international cybersecurity agencies. For example, representatives of the NSA have explicitly suggested that, "Nation States are robbing banks," and they're doing it with computers[103].

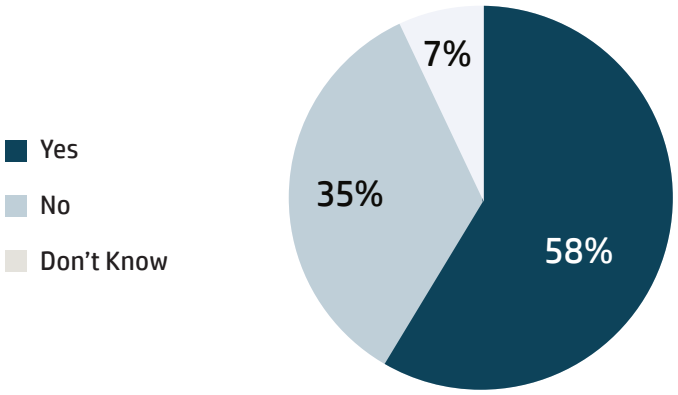
99 McGuire (2018)
100 Zetter (2016)
101 Schwartz (2018b)
102 Roth and Berlinger (2021)
103 Pollard (2017)

58% suggest it is not untypical for Nation States to recruit cybercriminals as proxies for cyberattacks.



Graph 3: Respondents' answers when asked if they believe that Nation States are making money from cybercrime

Our survey also suggested that many experts now suspect that Nation State and cybercriminal collusion is fairly commonplace, with 58% suggesting it is not untypical for Nation States to recruit cybercriminals as proxies for cyberattacks. The use of proxies, whether overtly cybercriminal or simply clandestine government agencies not only extends capability but allows for plausible deniability[104]. Robert Hannigan, the former head of GCHQ, has corroborated this suspicion, arguing that, "You can see these groups sitting in the same room, conducting state activity during the day, then crime at night. It's an interesting mixture of profit and political intent"[105].



Graph 4: Respondents' answers when asked if they believe Nation States are recruiting cybercriminals

Estimating the ***level*** of income that Nation States make from cybercrime is of course highly challenging, since reliable information that can be used to calculate it is extremely limited. What can be done, however, is to look at some specific kinds of illicit revenue streams like IP theft or cryptocurrency hacks and associate these with more conventional economic indicators to obtain some more educated estimates of the benefits of cybercrime to Nation State actors.

104 Maurer (2018b)
105 Schwartz (2018)

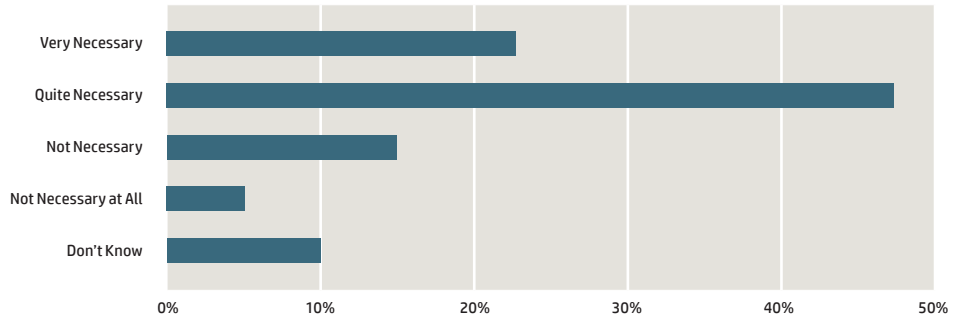
4.1

CYBERWAR AND CYBERPEACE

30% of our respondents remained sceptical about the prospect of any viable agreement or treaty.

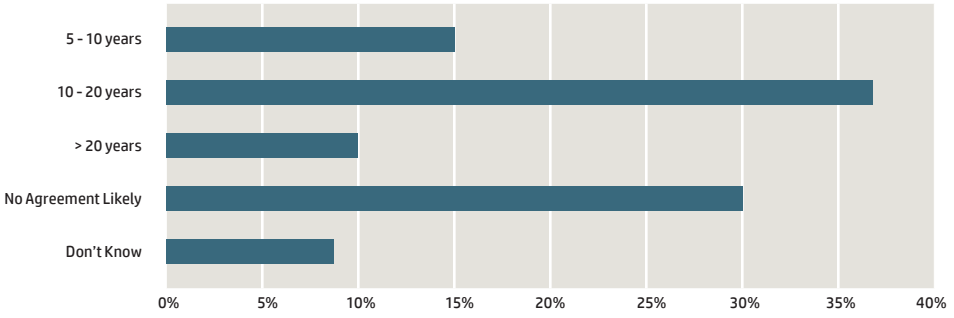
The previous sections have suggested how significant the risks which now confront us might be. On the one hand, the Advanced Cyberconflict Heat Gauge indicates how distinctions between (acceptable) cyber-competition and (unacceptable) forms of advanced conflict are blurring. On the other, our SOTTT analysis highlights an increasing range of links between sophisticated cyber tools and militaristic strategic objectives. As a result, there is a clear and present need to defuse any further escalations.

This concern was reflected in our survey, where **70%** of the experts agreed that some form of agreement or cyber-treaty is now essential if Nation States are to avoid being drawn into more serious forms of online conflict.



Graph 5: Respondents' answers when asked how necessary it is to create a cyber-treaty

When pressed on the likely timescale for any such agreement, the response was surprising. Most respondents (52%) thought it was likely within either the next 5-10 years or the next 10-20 years. One respondent pointed out that this timescale was plausible because it was "in the interests of all parties to move on defusing potentially more serious clashes." Another said, "if it doesn't happen, no-one is going to be ready for what will follow."



Graph 6: Respondents' answers when asked the most likely timescales for creating a viable cyber-treaty

But what form could any such agreement take? Would it involve one all-encompassing agreement, or a patchwork of differing treaties and/or conventions? Would it simply extend agreements governing conventional warfare, like the Geneva Convention? Or would it need to take on a form which is more cyber specific? Perhaps due to these complications, 30% of our respondents remained sceptical about the prospect of any viable agreement or treaty.

At minimum, a successful agreement would appear to depend upon convergence in two key factors:

(i) ***Scope.*** The parties included the range of jurisdictions involved and the specific kinds of activity covered.

(ii) ***Consensus.*** Agreement on the kinds of principles which should shape it. These may relate to prevention – such as weapons limitation – but also to the conduct of any cyberwar.

Taking these factors into consideration, we developed a chart (see table below) to indicate some of the options for agreement currently available to Nation States. These are not exhaustive but give an idea of the sort of building blocks which could be drawn upon for achieving consensus and de-escalating tension. The table covers two areas:

First, the kinds of agreement available for regulating conduct prior to the outbreak of more advanced forms of cyberconflict. Some of these are directed merely at securing better co-operation in cybersecurity or against cybercrime. Some are more overtly directed at conflict prevention.

Second, the kinds of agreement available for regulating conduct should more advanced forms of cyberconflict (a 'cyberwar') break out.

The table distinguishes between the scope of agreements at several levels, including: Domestic; Industry; and State / International based.

LEVEL	EXAMPLE OF CURRENT/ PROPOSED AGREEMENT	SCOPE	CONTENT
Standards of Conduct/Consensus prior to advanced cyberconflict			
Domestic	US Vulnerability Equities Process (VEP)	Transparency and co-operation between state and government agencies in reducing Nation State threats.	Requires the US Government and its agencies to disclose cyber vulnerabilities to leading companies like Apple, Cisco, Juniper, and Fortinet, whilst permitting intelligence agencies to retain information about zero-days.
Industry	Cybersecurity Tech Accord	Digital Tech Industry co-operation in reducing Nation State threats.	Aims to foster co-operation amongst digital technology companies to enhance the "security, stability and resilience of cyberspace" – especially against Nation State threats. Over 150 signatories, including HP, Facebook, Dell, BT, Microsoft, Hitachi, Panasonic, Cisco, Nokia, RSA & Orange.
Industry	Siemens Charter of Trust	Creation of industry standards for online safety against Nation State threats.	Aims to "set minimum general standards for cybersecurity", centred upon three goals for safer networks for individuals, companies and infrastructures: data protection; damage limitation; reliable foundations for trust.
Industry & States	Paris Call for Trust and Security in Cyberspace	Co-operation between industry and states in reducing Nation State threats.	Call to enhance international safety against malicious online activity; preventing interference in electoral processes; tightening up of online mercenary activities and offensive action by non-state actors; cooperating to enhance relevant international standards. Signed by 51 countries, 347 companies, including HP and 92 non-profit organisations, universities, and advocacy groups.
States / International	(Budapest) Convention on Cybercrime	Enhancing consensus and co-operation in fighting cybercrime to reduce Nation State threats.	Ratified by 65 States, the Convention aims to harmonise domestic law & policy towards online offending amongst signatory states. The Convention is oriented more towards crime than norms of conduct and key cyberpowers like Russia, China, India, Brazil have refused to sign up to it because of their strategic concerns.
States / International	(Proposed) UN Cybercrime Treaty	Enhancing consensus and co-operation in fighting cybercrime to reduce Nation State threats.	Proposed by Russia, China and others in early 2020. Following this, an ad hoc committee of experts, which represent all regions, has been scheduled for May 2021, to elaborate details on a 'comprehensive international convention on countering the use of information and communications technologies for criminal purpose'[106].
States / International	UN GGE Process	Creating consensus about norms of conduct in cyberspace.	UN Group of Governmental Experts (GGE), which aims to develop greater consensus between all member states on acceptable conduct and norms across digital networks.
Standards of Conduct/Consensus during advanced cyberconflict ('cyberwar')			
Combatants	Tallinn Manual 2.0	Creating standards for Nation State conduct during any advanced cyber conflict (cyberwar).	Composed by international legal experts under the auspices of NATO and intended as a reflection of law rather than a prescriptive guide. Focuses upon cyber-operations, rather than cyberwar in order to be applicable to broader nature of conflict (e.g. cognitive hacking). Considers how existing principles around issues including, "sovereignty, jurisdiction, due diligence, and the prohibition of intervention" might be applicable.

Table 4: Current/proposed frameworks for cyber-treaties

106 UN (2021)

4.2 NEW OPTIONS FOR A CYBERCRIME TREATY?

In 2020 what seemed to be an important development in the search for frameworks occurred when a new proposal for a 'cybercrime treaty' was put to the UN aimed at 'countering the use of information and communications technologies for criminal purposes'[107]. Though this was adopted by 79 votes to 60 with 33 abstentions[108], a lack of international consensus together with Nation State competition in realising strategic goals means that this initiative seems as unlikely to receive universal approval as the other indicated options.

The problem is that the proposal, which was sponsored by Russia and backed by China, would permit internet black-outs and the criminalisation of free speech. A group of NGOs and rights groups wrote to the UN to protest that the proposal would compromise rights as much as it combatted cybercrime (ibid.). And there is also the suspicion that it may simply be a move to replace the Budapest Convention with something more to non-signatories' liking.

More optimistically, the fact that Russia has been so active in drafting resolutions around information security to the UN General Assembly since 1998 offers hope that non-western nations may be serious about achieving a more fundamental cyberpeace. Russia was also instrumental in proposing moves on a UN Group of Governmental Experts (GGE) report in 2003 which could identify possible areas of cooperation for reducing cyberconflict. Despite a lack of support for this, a GGE report did emerge in 2010 recommending the international community develop and discuss norms and confidence-building measures[109].

4.3 CHALLENGES AND QUESTIONS

For any of these frameworks to prove viable, a range of challenges remain. For example:

(i) Striking the right balance between national security needs and the needs of enterprise looks to be precarious. For example, the US Vulnerabilities Equities Process looks to heavily favour governmental interests at present. Governance is in the hands of a Board chaired by the National Security Council (NSC) and attended by representatives from other agencies; including those most concerned with the security of critical US infrastructure, like the Department of Homeland Security and the Department of Commerce. Its decisions have created an ongoing saga about the way Government is concealing known vulnerabilities from industry, with around 45 vulnerabilities in the systems of companies like Apple and Microsoft retained each year.

(ii) Agreements like the Siemens Charter, which are meant to regulate the conduct of industry, remain very limited in scope with few clear principles behind them. They also require far more signatories from industry and more obvious sanctions if they are to be effective.

(iii) Similar qualms relate to more international facing frameworks, like the Paris Call. Conspicuously absent as signatories are key cyber superpowers like the US, Russia, China, Iran, Israel, and North Korea – without their agreement it is hard to see what influence such an agreement might have.

(iv) Fully global agreements are therefore essential, yet approaches such as the UN GGE process, are at best limited, at worst lacking in several significant dimensions. For

107 Hakmeh & Peters (2020)
108 Stolton (2020)
109 Barrera (2017)

> *it is also concerning that what does exist is so limited in scope and so lacking in consensus. It is also striking how many of available proposals deal with crime/cybercrime, rather than more traditional forms of political consensus.*

example, though some consensus has been reached on issues like respect for human rights in cyberspace, there are many other key issues where there is no agreement, yet. Major questions also remain about what should govern state responsibility in cyberspace and their right to self-defence.

The fact that any agreements – albeit only in the form of outlines – are in place at all perhaps offers some hope that escalations into advanced cyberconflict may yet be avoided.

However, it is also concerning that what does exist is so limited in scope and so lacking in consensus. It is also striking how many of available proposals deal with crime/cybercrime, rather than more traditional forms of political consensus. This perhaps corroborates the observation made in this report that we have arrived at a wholly new state of international relations, one where crime and politics have become mixed in subtle ways.

At least ten key questions therefore remain which will need to be addressed in the coming years if a continuing spiral into something like a cyberwar (or worse) is to be halted:

(i) How can existing agreements be transformed from symbolic statements of intent into anything more binding upon the signatories?

(ii) Will it be possible for the cyber superpowers involved in driving much of the online conflict studied in this report to ever engage in serious commitments to conflict reduction?

(iii) Can ways be found of preventing regional cyberconflicts from spilling onto the global stage?

(iv) How can issues around global cyber-criminality be disentangled from issues around global strategic interest? In particular, what kinds of restrictions on the use of cybercriminal tools and techniques should there be?

(v) What are the liabilities of cyber-proxy groups and what restrictions on the use of cyberweaponry should there be? Is any form of 'arms reduction' possible?

(vi) Should attempts to forge consensus be driven at the supranational level or by more grass roots activists?

(vii) What kinds of verifications for an agreement could be put in place and what agency could be accepted to arbitrate violations?

(viii) What duties or protections to civilians will be considered?

(ix) Is any system of compensation for harms suffered as a result of cyberconflict viable?

(x) What responses could there be if anything should or could happen where lines are crossed – could there be 'cyberwar crimes'?[110]

110 RAND (2019)

5.1

CONCLUSIONS AND RECOMMENDATIONS

On the evidence of this research, we are at a significant tipping point in the way Nation States use information technology. Nation States across the political divide appear increasingly ready to use cyberspace aggressively, often with little apparent concern for the consequences.

As a result, an increasingly wide range of victims seem likely to be caught up in the crossfire. Whole cities and municipal districts face network shutdowns, ransom demands and data losses as the result of shadowy groups; many of whom are acting as proxies for states. As critical infrastructure is targeted, we risk the merging of the cyber and physical worlds, with potentially catastrophic consequences that could result in loss of life. As media and information systems are targeted, it becomes harder to separate fact from fiction, or to make properly informed judgements about the direction our democracies should take. And as some Nation States' respect for law disappears, individuals face the use of information technology for wholesale monitoring, coercive control and – where they have been considered to challenge the power of Nation States too closely – cyber-targeted assassination itself.

Any suggestion that the balance may be tipping towards more advanced forms of cyberconflict is therefore of concern to us all – not just stakeholders in the practice of cybersecurity. Of equal concern then is the role played in all this by the draw upon the Web of Profit associated with the burgeoning cybercrime economy. Within this $1.5 trillion economy, Nation States not only directly and indirectly profit from cybercriminality, they also seem ready to use cybercrime tools and technique to bolster military capacity or to even employ criminal groups to further their strategic objectives.

The resulting blend of conflict and crime we now face is surely unprecedented and heralds an uncertain future for the information society. For any entry of relations more typical of crime into the arena of international relations – in particular, a disrespect for the rule of law – risks creating a state of perpetual (though undeclared) conflict, which may be impossible to untangle.

With this in mind, this research suggests a range of recommendations that might be applied:

(i) Policy makers need to engage more actively in the pursuit of cyber-treaties and cyber-agreements.

(ii) For such treaties to be effective, there needs to be a wider recognition of legitimate Nation State interests in cyberspace, a recognition which is not overly shaped by individual Nation State strategic objectives.

(iii) International law enforcement agencies need to help to disrupt the flow of Nation State driven forms of cybercrime revenue generation.

(iv) International financial authorities should engage more actively in attaining co-operation between Nation States in addressing actions which foster Nation State cybercrime, such as money laundering.

(v) Cybersecurity professionals need to be more active in building up intelligence around typical Nation State cyberweapons and in finding ways of combating these.

(vi) Enterprise should co-operate to develop more proactive forms of managing Nation State threats to their data and network capacity.

(vii) Individual citizens should engage more actively in pressing their governments to find ways of cooperating in cyberspace.

“

Nation States across the political divide appear increasingly ready to use cyberspace aggressively, often with little apparent concern for the consequences.

“

As critical infrastructure is targeted, we risk the merging of the cyber and physical worlds, with potentially catastrophic consequences that could result in loss of life.

“

Within this $1.5 trillion economy, Nation States not only directly and indirectly profit from cybercriminality, they also seem ready to use cybercrime tools and technique to bolster military capacity or to even employ criminal groups to further their strategic objectives.

BIBLIOGRAPHY

Abrams, L., 2021, Solar Leaks site claims to sell data stolen in SolarWinds attacks, Bleeping Computer, 12/01/2021

Accenture, 2020 Cybersecurity Report

Ashford, W., 2018, Cyber criminals catching up with Nation State attacks, Computer Weekly, 26/02/2018

Ball, J., 2013, NSA monitored calls of 35 world leaders after US official handed over contacts, Guardian, 25/10/2013

Barrera, M., 2017, The Achievable Multinational Cyber Treaty, Air University Press

BBC, 2015, China denies Australia Bureau of Meteorology 'hack', 02/12/2015

BBC, 2019, Australian political parties hit by 'state actor' hack, PM says, 16/02/2019

BBC, 2019b, German politicians targeted in mass data attack, 04/01/2019

BBC, 2021 Trump bans Alipay and seven other Chinese apps, 06/01/2021

Bosetta, M., 2018, The Weaponization of Social Media: Spear Phishing and Cyberattacks on Democracy, Columbia Journal of International Affairs, 20/09/2018

CFR, 2019, Cyber Operations Tracker, Council on Foreign Relations

Chandler, S., 2020, Google Registers Record Two Million Phishing Websites In 2020, Forbes 25/11/2020

Coker, J., 2020, Attacks on Pharma Rise Amid Targeting of #COVID19 Vaccine Development, Infosecurity, 19/11/2020

Corera, J., 2016, How France's TV5 was almost destroyed by 'Russian hackers' BBC 10/10/2016

Coughlan, S., 2020 Cyber threat to disrupt start of university term, BBC 17/09/2020

Crerar, P., Henley, J., & Wintour, P., 2018, Russia accused of cyberattack on chemical weapons watchdog, Guardian, 04/10/2018

Crowdstrike, 2019, 2019 Global Threat Report

CSIS, 2020, Significant Cyber Incidents, Center for Strategic and International Studies

Cushing, T., 2019, Chinese Spies Intercepted NSA Malware Attack, Weaponized It Against Targets Around The World, Techdirt, 08/05/2019

D'mello, A., 2019, Threat intelligence report shows new IoT vulnerabilities, Nation State actors and a rise in DDoS frequency, Vanilla Plus, 28/02/2019

DeVore, M., & Lee, S., 2017, APT (advanced persistent threats) and influence: cyber weapons and the changing calculus of conflict The Journal of East Asian Affairs, 31, 1pp. 39-64

Doffman, Z., 2020, Twitter Confirms 'Nation-State' Attack, Forbes, 04/02/2020

Elkind, P., 2015, Sony Pictures: Inside the Hack of the Century, Fortune, 27/06/2015

Elliott, C., 2019, Here Are The Real Fake News Sites, Forbes, 21/02/2019

ENISA, 2019, Shamoon Campaigns with Disttrack, European Union Agency for Cybersecurity, 07/01/2019

ENISA, 2020, Cyber espionage, ENISA Threat Landscape, 01/2019-04/2020

FireEye, 2019, M-Trends 2019 Special Report

GFI, 2019, Global Firepower index, see: https://www.globalfirepower.com/countries-listing.asp

Goodin, D., 2019, Unkillable LoJax rootkit campaign remains active, Arstechnica, 16/01/2019

Gov.uk, 2018, UK exposes Russian cyber attacks, Press Release, 04/10/2018

Greenberg A., 2017, Your Guide to Russia's Infrastructure Hacking Teams, WIRED, 12/07/2017

Guglielmi, G., 2020, The next-generation bots interfering with the US election, Nature, 28/10/2020

Hakmeh, J., & Peters, A., 2020, A New UN Cybercrime Treaty?, Council on Foreign Relations, GuestBlog, 13/01/2020

Hall, K., 2018, Brit Attorney General: Nation State cyberattack is an act of war, The Register, 23/05/2018

Hegre et al., 2011, Predicting Armed Conflict, 2010–2050 International Studies Quarterly 57(2): 250–270

Hern, A., 2016, Ukrainian blackout caused by hackers that attacked media company, researchers say, Guardian, 07/01/2016

Herr et al., 2020, Breaking trust: Shades of crisis across an insecure software supply chain, Atlantic Council, 26/07/2020

Hoffman, K., 2019, True crime: SamSam ransomware I am, SC Media, 01/02/2019

Ignatius, D., 2018, How a chilling Saudi cyberwar ensnared Jamal Khashoggi, Washington Post, 18/12/18

Izvestia, 2020, Russia will increase spending on information security, 02/10/2020

ITRC, 2020, Data Breach Report, Identity Theft Resource Center

Jackson and Morelli, 2009, The Reasons for Wars – an Updated Survey, in Handbook on the Political Economy of War, edited by Chris Coyne, Elgar Publishing

Jay, J., 2020, Microsoft issues fresh warning about Nation State actor Gadolinium, Teiss, 25/09/2020

Jones, C., 2018, EU communications hack linked to Chinese spies, ITPro, 19/12/2018

JTA, 2019, Israel's national broadcaster accuses Hamas of Eurovision hack, Jewish News, 18/05/2019

Katwala, A., 2018, Why China's perfectly placed to be quantum computing's superpower, WIRED, 14/11/2018

Kirschgaessner, S., 2020, Jeff Bezos hack, The Guardian, 22/01/2020

Korolov, M., 2021, What are Supply Chain Attacks, and How to Guard Against Them, DataCenter Knowledge, 12/01/2021

Krebs, B., 2021, SolarWinds: What Hit Us Could Hit Others, Krebs on Security, 12/01/2021

Kundaliya, D., 2019, Russian state-sponsored attackers take just 20 minutes to infiltrate networks, claims CrowdStrike, Computing, 20/02/2019

Lancaster, K., 2020a, 10 facts about Nation State cyberattacks, ID Agent, 19/11/2020

Lancaster, K., 2020b, Sudden Spike in Healthcare Cyberattacks May Be Nation-State Hackers, ID Agent, 29/10/2020

Lewis, P., & Unal, B., 2019, The Destabilizing Danger of Cyberattacks on Missile Systems, Chatham House, Expert Comment, 02/07/2019

Leyden, J., 2019, Chinese cyber spies 'target international businesses to pilfer trade secrets', Daily Swig, 07/02/2019

Lightcyber, 2016, Cyberweapons 2016 Report

Lucero, L., 2018, F.B.I.'s Urgent Request: Reboot Your Router to Stop Russia-Linked Malware, New York Times, 27/05/2018

Maurer, T., 2018a, Why the Russian Government Turns a Blind Eye to Cybercriminals, Slate, 02/02/2018

Maurer, T., 2018b, Cyber Mercenaries: The State, Hackers, And Power, New York and Cambridge: Cambridge University Press.

Maxwell, P., 2017, Stockpiling Zero-Day Exploits: The Next International Weapons Taboo, 2th International Conference on Cyber Warfare and Security, Dayton, OH March 2017

McGuire, M., 2018, Into the Web of Profit, Bromium, 20/04/2018, see https://www.bromium.com/resource/into-the-web-of-profit/

McGuire, M., 2019, Into the Web of Profit: Behind the Dark Net Black Mirror, Bromium, 05/06/2019, see https://www.bromium.com/resource/into-the-web-of-profit-behind-the-dark-net-black-mirror/

Merriman, C., 2019, Amazon's Jeff Bezos was hacked by Saudi Arabia, investigation finds, Inquirer, 01/04/2019

MIT, 2019, Atlas of Economic Complexity, accessible at: https://oec.world/en/

Muncaster, P., 2017, EU to Declare Cyber-Attacks "Act of War", Infosecurity, 31/10/2017

Muncaster, P., 2020, Russian APT28 Group Changes Tack to Probe Email Servers, Infosecurity, 20/03/2020

Nakashima, E., 2019, At nations' request, US Cyber Command probes foreign networks to hunt election security threats, Washington Post, 07/05/2019

NCSC, 2018a, Preventing Lateral Movement, UK National Cybersecurity Centre, Advisory note, 08/02/2018

NCSC, 2018b, APT10 continues to target UK organisations across wide range of sectors, Alert, 20/12/2018

NCSC, 2020, NCSC defends UK from more than 700 cyber attacks, News item, 03/11/2020

Howell O'Neill, P., 2018, Drones emerge as new dimension in cyberwar, Cyberscoop, 05/02/2018

O'Malley, M., 2020 Concerned about Nation State Cyberattacks?, Security Magazine, 26/03/2020

Osbourne, C. 2016, Dark Web drugs, data dumps and death: Which countries specialize in what services?, ZDNet, 02/03/2016

Perlroth, N. & Shane, S., 2019, In Baltimore and Beyond, a Stolen N.S.A. Tool Wreaks Havoc, New York Times, 25/05/2019

Pollard, N., 2017, Ghosts in the Machine that Can Rob You Blind, The Cipher Brief, 03/12/2017

RAND, 2019, Accountability in Cyberspace: The Problem of Attribution, 14/04/2019

Reuters, 2019, Government officials around the globe targeted for hacking through WhatsApp – sources, 31/10/2019

Reuters, 2021, Suspected Chinese hackers used SolarWinds bug to spy on U.S. payroll agency, 02/02/2021

Robertson, R., 1994, Globalisation or glocalisation? The Journal of International Communication 1, pp 33-52

Roth and Berlinger, 2021, North Korean hackers stole more than $300 million to pay for nuclear weapons, says confidential UN report , CNN, 09/02/2021

RTS, 2016, The hackers stalking TV networks, Royal Television Society, November 2016

Schwartz, M., 2018a, Cybercrime Groups and Nation State Attackers Blur Together, BankInfo Security, 18/06/2019

Schwartz, M., 2018b, Lazarus 'FASTCash' Bank Hackers Wield AIX Trojan, BankInfo Security, 12/11/2018

Seal, T., 2021, Microsoft Exchange Zero-Day Attackers Spy on U.S. Targets, Threatpost, 03/03/2021

Shane, S., 2018, Russia Isn't the Only One Meddling in Elections. We Do It, Too, New York Times, 17/02/2018

Sherman & Zoob, 2018, The Triton Cyber Weapon, RealClearDefense, 04/04/2018

Silverman, C., 2016, This analysis shows how viral fake election news stories outperformed real news on Facebook, Buzzfeed News, 16/11/2016

Simmons, D. 2019, Cyber-attacks 'damage' national infrastructure, BBC 05/04/2019

Slye, J., 2020, The FY 2021 Federal Budget Sustains Cybersecurity Funding, Govwin

Smith, M., 2015, Researchers link QWERTY keylogger code to NSA and Five Eye's Regin espionage malware, CSO, 27/01/2015

Snoddy, R., 2016, The hackers stalking TV networks, Television Magazine, November 2016

SOFF, 2017, State sponsored cyber attacks, Swedish Security and Defence Industry Association

South, T., 2018, New cyber weapons are here and no one is prepared, experts say, Army Times, 09/04/2018

Stewart, R., 2019, Chinese-linked APT10 adds new Quasar RAT and PlugX variants to its arsenal Cyware, 28/05/2019

Stolton, S., 2020, UN backing of controversial cybercrime treaty raises suspicions, Euractive, 23/01/2020

Sun Tzu, 2018, The Art of War, CreateSpace Independent Publishing

Symantec, 2019 Internet Security Threat Report 2019

Tannam, E., 2018, GitHub falls victim to world's largest DDoS attack: What you should know, Silicon Republic, 02/03/2019

Thomson, I., 2017, Everything you need to know about the Petya, er, NotPetya nasty trashing PCs worldwide, The Register, 28/06/2017

UN, 2021, Ad hoc committee established by General Assembly resolution 74/247: Postponement. See: https://www.unodc.org/unodc/en/cybercrime/cybercrime-adhoc-committee.html

Uren, T., Hogeveen, B., Hanson, F. et al., 2018, Defining offensive cyber capabilities, Australian Strategic Policy Institute, 04/07/2018

Voo, J. et al., 2020, National Cyber Power Index 2020, Harvard College, available at: https://www.belfercenter.org/sites/default/files/2020-09/NCPI_2020.pdf

Walden, P. & Kashefi, E., 2019, Cyber Security in the Quantum Era. Communications of the ACM, April 2019, 62, 4, p. 120

Wall, M., 2018, Is this the year 'weaponised' AI bots do battle?, BBC, 05/01/2018

Wolfe, D., 2019, A cyberattack in Japan could now bring the US into war, Quartz, 20/04/2019

Xinhua, 2019, China to lead global cybersecurity market growth in next 5 years, China.org.cn, 09/09/2019

Zetter, K., 2016, That Insane, $81M Bangladesh Bank Heist? Here's What We Know, WIRED, 17/05/2016

APPENDIX – METHODOLOGY

The scarcity and lack of reliability when researching online conflicts between Nation States is well known and predictable given the sensitivities here. A great deal of data is classified by national governments and therefore inaccessible to researchers, and even where data is available it must be handled with care and a certain amount of scepticism. If a Nation State is content with information not being made available, one has to ask why, and who it benefits. Also, it is worth noting that the kind of information that is available to researchers in western societies is heavily slanted towards interests there. In many ways we know more about Russian and Chinese cyber operations than we do about US or UK parallels.

The study drew upon four main sources of information:

(i) Well documented reports in the public domain obtained from secondary sources, whistle-blowers and insider leaks.

(ii) Expert insight obtained from a survey of 50 leading practitioners in relevant fields. These included:

UK Law enforcement	5 respondents
European and International Law Enforcement	5 respondents
Government	4 respondents
Intelligence	6 respondents
Cybersecurity	10 respondents
Media & Journalism	5 respondents
NGOs	5 respondents
Academia	10 respondents

Because of the sensitivity of the issues covered in the report, responses were only provided on the basis of anonymity and non-attributabilit.

(iii) Informal, non-structured interviews with informants across the dark net and other covert sources.

(iv) Inductive analysis of around 200 incidents which have been reliably associated with online Nation State struggles.[111]

Insights from the raw, and often limited secondary data which is available were enhanced by new analytic tools designed to 'fill in the gaps' with as reliable a range of inferences as possible. For example, the NSiC (Nation States in Cyberspace) approach helped break down the complexities of Nation State cyberconflict into four key patterns defined as 'SOTTT' variables.

S – The ***strategies*** being developed by Nation States to attain superiority in cyberspace

O – The ***objective*** of Nation States in seeking strategic advantage

T – The main ***targets*** of these struggles

T – The major ***tools*** (cyber weapons)

T – ***Techniques*** (attack vectors) being used by Nation States for these purposes

111 The list of incidents assembled for this research drew upon two existing databases (see CSIS 2020 & CFR 2019), potential Nation State attacks mentioned in other secondary sources and off-the-record observations from experts consulted during this research

HP WOLF SECURITY