TOP TRENDS TO CONSIDER

UNDERSTANDING CRIMINAL CYBER THREAT ACTORS AND MOTIVATIONS

CyberCube

Every year, a considerable amount of research is authored to raise levels of awareness concerning cyber security attack methods, criminal trade-craft and possible outcomes resulting from malicious activity. In our view, not enough of this research focuses on the threat actors carrying out these attacks.

This report builds on some of the trends highlighted in CyberCube's *Global Threat Briefing: threat actor activity update and predictions for H1 2022*, focusing in more detail on nation-state attacks and criminal gangs.

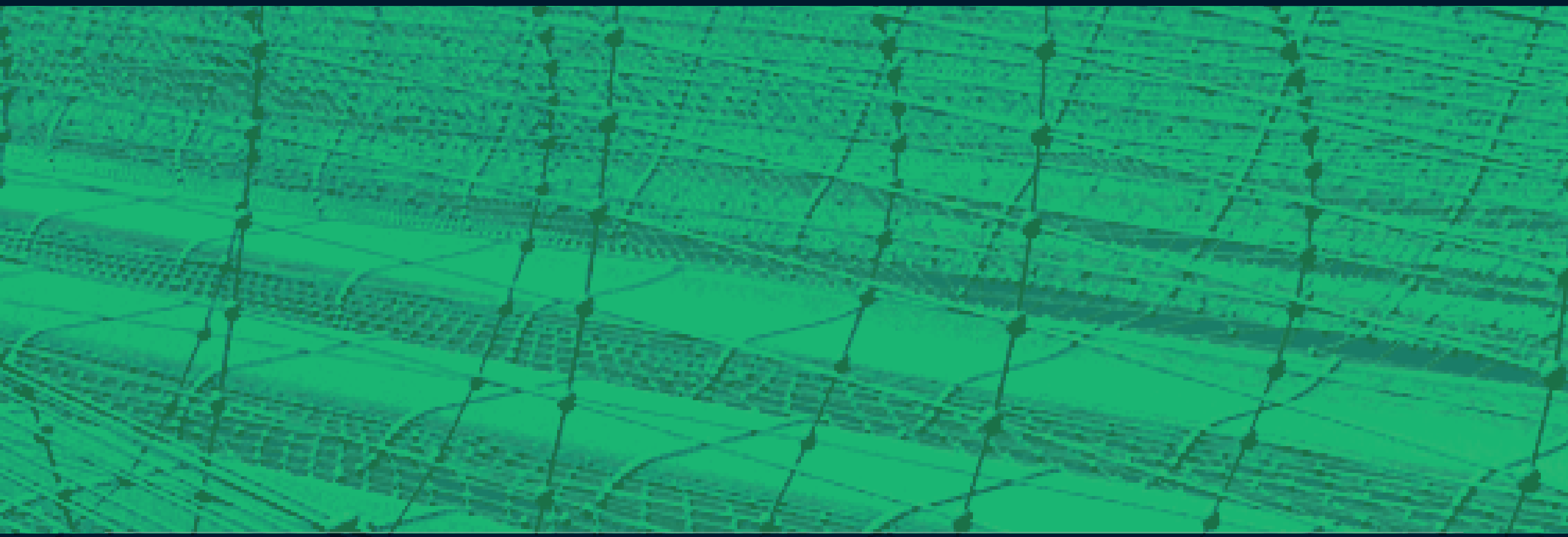
DOWNLOAD NOW

In this report, we also explore the complex relationship between nation states and criminal communities. A greater understanding of the key cyber actors, their motivations, and how these lead to the utilization of specific techniques will help (re)insurers and brokers predict how and where future attacks could arise and inform estimations of attack frequency and severity. CyberCube has issued this paper with these objectives in mind. We remain committed to researching and publishing up-to-date information on cyber threat actors, and readers should consider this paper as an introduction to themes and topics concerning cyber security threat actors that we will return to in future publications.

TYPICAL THREAT ACTORS AND THEIR MOTIVATIONS

It is important to recognise that cyber threat actors can take many forms, including those that, from a Western political perspective, are deemed to be lawful. For example, members of the "Five Eyes Alliance", an intelligence-sharing partnership set up after World War II and comprising the US, Canada, the United Kingdom, Australia and New Zealand, could be categorized as a body of "threat actors" by countries upholding a different political perspective. These nation states (often in collaboration) are certainly active in cyber and, conceivably, carry out cyber operations designed to disrupt or, at the very least, derive intelligence from other nation states. This paper focuses on actors with whom the insurance industry should concern itself because they are most likely to inflict cyber attacks on Western democracies and businesses and create systemic risk that leads to risk aggregation and large financial losses.

These types of threat actors can be categorised as state-sponsored actors, organized criminal gangs, and hacktivists.



STATE-SPONSORED ACTORS

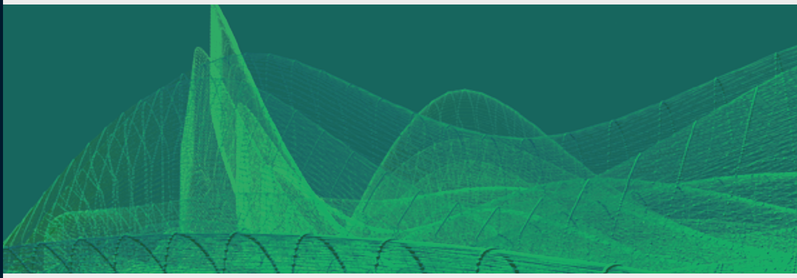
The mechanisms and levels of support to criminals from state sponsorship are complicated, and a specific section of this document ("The spectrum of state sponsorship") has therefore been dedicated to this topic.

These threat actors are among the most significant and concerning to the (re)insurance industry and potential victims of cyber crime. State-sponsored actors are affiliated with government entities and, as a result, tend to represent well funded, well organized and sophisticated actors with mature procedures, and with the blessing of (and, therefore, with protection from) an associated government.

State-sponsored actors' objectives also tend to align with the government entity that sponsors them. Generally, therefore, state-sponsored attacks that we have witnessed in the past have been politically motivated, often gearing their efforts towards espionage. Other campaigns seen from these actors have included distributed denial of service (DDoS) attacks, destructive wiper malware, misinformation, influence operations, and attacks on critical infrastructure.

In addition, attacks carried out on behalf of nation states tend to be more strategically focused than pure criminal attacks, often playing out over months or even years. Strategically focused activities often focus on advancing a political agenda rather than simply generating financial benefit for the actor.

The most destructive nation-state sponsored attack in recent years was the NotPetya ransomware outbreak in 2017. Russian military hacking groups allegedly deployed the NotPetya malware to target Ukrainian entities, but the effect became global almost instantaneously. Damage from NotPetya affected global shipping companies, multi-national pharmaceutical companies, financial services organizations, and food manufacturers. Some estimates suggest that it caused $10 billion in damage.



State-sponsored actors have been responsible for some of the most high-profile cyber attacks in recent history. Russian state actors were responsible for conducting an attack on SolarWinds in 2020, which they used to breach a variety of US federal agencies including NASA. However, Russian state actors are not the only state-sponsored threats to worry about. Chinese military actors were responsible for an attack against Microsoft Exchange, which resulted in a global wave of cyber attacks and data breaches beginning in January 2021. Looking at the cyber threat landscape today, a growing array of state actors from Iran to North Korea and others are increasingly active.

ORGANISED CRIMINAL GANGS

There is no doubt that well-executed cyber crime can be lucrative for criminals. Cybersecurity Ventures estimates that global damage related to cyber crime will reach $10.5 trillion by 2025. Over the past ten years, the cyber crime landscape has evolved rapidly from a few sophisticated criminal gangs and thousands of individuals operating on a "best efforts" basis to a mature global eco-system comprising well-organized company structures and mature software supply chains. Organized cyber criminals are motivated by financial gain and trends seen in cybercrime always reflect where the most profit can be made for the least effort. Today, this is ransomware - locking up a victim's data and demanding a ransom payment to decrypt the data - and this particular technique for extracting profit shows no signs of abating.

In fact, ransomware gangs are evolving their tactics, techniques, and procedures at a rapid rate. The more evolved and mature criminal gangs have turned their attention in recent years to providing sophisticated hacking tools to other, affiliate cyber criminal gangs via a software-as-a-service distribution method. This is known as ransomware-as-a-service (RaaS) and, through this method, the larger players lessen their risk whilst generating significant profits from the criminal ecosystem, and less mature actors are able to obtain sophisticated ransomware toolkits for a relatively small initial investment.

Today, one of the most well-known cyber criminal operations is Wizard Spider. By their very nature, criminal gangs are hard to trace and identify, but researchers suggest that Wizard Spider, based in St. Petersburg, Russia and active since 2016, has authored hacking tools and malware including TrickBot, Ryuk, Conti and BazarLoader. These represent some of the most sophisticated and dominant ransomware loaders and strains seen so far in the wild.

HACKTIVISTS

Hacktivists are individuals or groups who use hacking to effect political or social change. These actors carry out political activism, leveraging the Internet to create impact, and using security vulnerabilities to affect their targets. The hacktivist landscape is somewhat less well-defined and organized than the cyber criminal landscape, encompassing individuals and groups with various levels of skill sets and capabilities. Modern hacktivism has been shaped by a few major players in this space over the past decade. One of the most influential of these has been the Anonymous group, which has taken on many political causes since its inception, ranging from support for the Black Lives Matter movement to support for Ukraine in the 2022 Russia-Ukraine conflict. Anonymous is made up of proxy organizations, making it difficult to track and properly attribute attacks to the group. However, groups like Anonymous often take public credit for their attacks.

The more influential hacktivists do present a very real threat to business and to the cyber insurance market. These organizations play a very dangerous game when putting state secrets and intelligence operations in harm's way and the potential repercussions of these activities are far reaching. Anonymous recently hacked the Russian Central Bank, releasing 28GB of data exfiltrated from the bank in direct response to Russia's activities in Ukraine. The data leaked by Anonymous included invoices, internal communications, documents, notes, bank statements, shareholder names of various banks, bank licenses and the names and addresses of high-profile clients.

NATION-STATE ACTORS AND RECENT TRENDS

CyberCube expects to see more activity from nation-state cyber threat actors in the coming years. The number of nation states who now see cyber capability as key to their strategic, national objectives is increasing, and many nation states are maturing their capabilities at a rapid pace.

Of particular interest to insurers are nation-state actors who tend to show high degrees of persistence and sophistication in their attacks. We often refer to these actors as advanced persistent threats (APTs). APTs are rising in number, operating simultaneously and often competitively. APTs will be focused on compromising specific adversaries, as well as waging espionage and intelligence campaigns.

CYBERCUBE NOTES THE FOLLOWING TRENDS IN THIS AREA IN 2022:

Espionage attacks are currently still more prevalent than destructive attacks

The most common targets include governments, non-governmental organizations (NGOs), think tanks, key intellectual property (IP) and public utilities

More nation-state threat actors are seen to be financially motivated, focusing on IP theft and ransom payments

The top 1% of APTs are compromising supply-chain Single Points of Failure (SPoF) to impact downstream customers en-masse

Enterprises are not safe from nation-state threats and often end up as collateral damage.

A **SPoF** is a provider which may disrupt large swaths of companies that rely on them for their business operations if they experience an outage. As the world becomes more highly interconnected and cyber risk is a growing problem, CyberCube has modeled hundreds of SPoFs and also enables analysis of over 20,000 unmodeled SPoF risks

Espionage attacks currently dominate, as nation-state actors have been focusing on intelligence collection, rather than destructive attacks. CyberCube expects this trend to continue and is monitoring regional hotbeds of cyber conflict, including those of Israel vs. Iran, India vs. Pakistan, Russia vs. Ukraine, and China vs. Japan, for indications that the boundaries of acceptable behavior are being pushed beyond historic precedent *(see Exhibit 1)*. Cyber-physical conflicts that could involve destruction include Iran becoming willing to engage in destructive attacks against Israel and Saudi Arabia (as was seen in the Shamoon attack of 2012). Recent Russian nation-state cyber attacks on Ukrainian organizations as part of its war effort have focused on disruption to business and critical infrastructure.

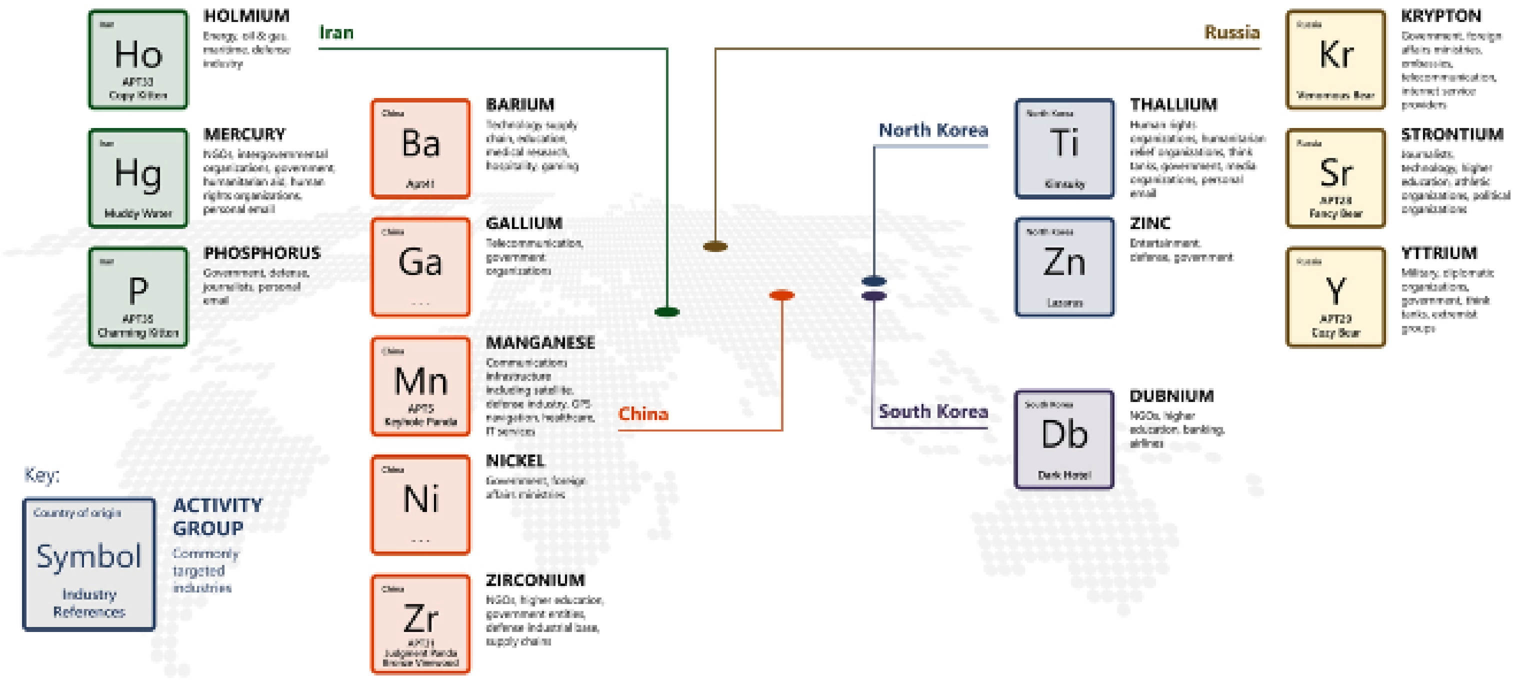
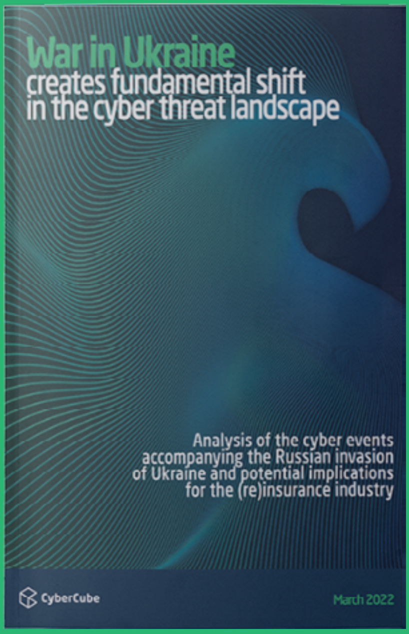

Iran
Ho
APT33
Copy Kitten
HOLMIUM
Energy, oil & gas, maritime, defense industry
Iran
Hg
Muddy Water
MERCURY
NGOs, intergovernmental organizations, government, humanitarian aid, human rights organizations, personal email
Iran
P
APT35
Charming Kitten
PHOSPHORUS
Government, defense, journalists, personal email
Iran
China
Ba
Apt41
BARIUM
Technology supply chain, education, medical research, hospitality, gaming
China
Ga
GALLIUM
Telecommunication, government organizations
China
Mn
APT5
Keyhole Panda
MANGANESE
Communications infrastructure including satellite, defense industry, GPS navigation, healthcare, IT services
China
Ni
NICKEL
Government, foreign affairs ministries
China
Zr
APT31
Judgment Panda
Bronze Vinewood
ZIRCONIUM
NGOs, higher education, government entities, defense industrial base, supply chains
China
Russia
North Korea
North Korea
Ti
Kimsuky
THALLIUM
Human rights organizations, humanitarian relief organizations, think tanks, government, media organizations, personal email
North Korea
Zn
Lazarus
ZINC
Entertainment, defense, government
South Korea
South Korea
Db
Dark Hotel
DUBNIUM
NGOs, higher education, banking, airlines
Russia
Kr
Venomous Bear
KRYPTON
Government, foreign affairs ministries, embassies, telecommunication, internet service providers
Russia
Sr
APT28
Fancy Bear
STRONTIUM
Journalists, technology, higher education, athletic organizations, political organizations
Russia
Y
APT29
Cozy Bear
YTTRIUM
Military, diplomatic organizations, government, think tanks, extremist groups
Key:
Country of origin
Symbol
Industry References
ACTIVITY GROUP
Commonly targeted industries

EXHIBIT 1

An increasingly crowded nation-state threat actor landscape (Source: Microsoft Digital Defense Report)

The monitoring of regional conflict enables understanding of adversarial innovations that are eventually likely to be used globally. As this report goes to press, we are already witnessing this play out in attacks emanating from Russia and targeting IT infrastructure in Ukraine. There is a high level of expectation that these attacks will extend to Ukraine's political allies in the West, probably sponsored by the Russian state and involving criminal gangs and hacktivists. Potential industries to be targeted have been highlighted in CyberCube's report ***War in Ukraine***.


War in Ukraine creates fundamental shift in the cyber threat landscape

Analysis of the cyber events accompanying the Russian invasion of Ukraine and potential implications for the (re)insurance industry

CyberCube

March 2022

DOWNLOAD NOW

Common nation-state targets include governments, NGOs and think tanks. As an example, vaccine research think tanks hold some of the most targeted IP of any institution recently as a direct consequence of the COVID-19 pandemic. Threat actors exploit the connections between the more traditional NGO community and government organizations to establish a presence and eventually gain insights into national policy plans and intentions. Think tanks with ideas relevant to current or future government policy or political objectives are in the threat actors' crosshairs.

Nation-state threat actors that are financially motivated remain in the minority for now. However, CyberCube has witnessed a trend that suggests that more nation-state actors are turning to cyber initiatives, incentivised by monetary gain. In these instances, actors are likely to steal IP and make ransom demands. Examples of nation-state actors include North Korea and Iran. Following years of economic sanctions, North Korea and Iran have sought alternative revenue streams, using cyber attacks to this end. As the war in Ukraine continues and Western sanctions punish the Russian state, we should expect Russian actors to use cyber attacks to both damage Western infrastructure and to make up for some of the financial losses caused by sanctions.

The top 1% of cyber threat actors are targeting IT service providers to improve their success in exploiting victims downstream who receive services from those providers. Key examples of this strategy to compromise supply-chain SPoFs are the Russian SolarWinds attacks and the Chinese exploitation of a vulnerability in on-premises Microsoft Exchange servers.

Enterprises are not safe from nation-state threats and often end up as collateral damage. In a recent example of a SPoF cyber attack, Russian state actors conducted an attack on the American satellite communications company Viasat. The goal of the attack was to disable the Ukrainian military's satellite communications at the start of the war. However, the attack had unintended consequences which included taking down Internet connectivity for tens of thousands of users throughout Europe and inadvertently shutting down 5,800 wind turbines in Germany.

CRIMINAL ACTORS AND RECENT TRENDS

Ransomware-as-a-service (RaaS) affiliates are under pressure to access and attack as many networks as possible and to access brokers (criminals who specialize in initial network intrusion) who have emerged to fulfil a critical role in the ransomware supply chain. These brokers sell access to networks and systems for others to attack. In 2020, Positive Technologies identified 707 new advertisements for sale of access - a sevenfold increase in the number of new advertisements compared with 2019. As many as 590 new offers were found in the first quarter of 2021 alone.

Access brokers are also scaling their operations with help from the operators of the world's biggest botnets. Botnets are armies of attacker-controlled computers that can serve as platforms for cyber attack operations. This includes gaining initial access to a network to drop other malware such as ransomware. Botnet malware proved to be the biggest malware threat to organizations in 2021, with an average of 8% of organizations globally being attacked on a weekly basis. Insurers should expect this trend to continue, along with other means of streamlining the process of cyber attack.

Ransomware threat actors are also becoming more innovative in terms of techniques. “Double extortion”, where data is not just encrypted but also stolen and mirrored to hold people and companies to ransom after the attack, has become commonplace. CyberCube expects attacks will focus increasingly on data integrity and authenticity in future, with data not just encrypted but altered to become unusable or untrustworthy. For example, a medical supplier could come under attack with altered drug recipes.

A FEW OTHER TRENDS IN RANSOMWARE ARE NOTABLE TODAY:

1. There are now over 50 RaaS variants in use, but the Conti variant is currently dominant, infecting almost twice as many victims as its nearest rival

2. Most ransomware attacks still occur in the US However, as these groups continue to scale and proliferate, CyberCube expects to see the internationalization of RaaS in 2022

3. More is known about criminal actors than ever before through the careful study of the many attacks that occur. In addition, recent data leaks from the criminal actors themselves have furnished the cyber security community with hitherto unknown information concerning ransomware threat actors and their techniques

4. Law enforcement actions are dissuading threat actors from staging “newsworthy” attacks, driving changes in criminal behavior, in terms of their targets.

RANSOMWARE TOOLKITS AND INFECTIONS

CyberCube's single-risk underwriting solution Account Manager equips cyber underwriting teams with the ability to identify pre-breach and post-breach indicators of compromise (IOCs) on a company's network. These IOCs include but are not limited to: (1) the identification of toolkits that can be used to drop ransomware onto a device/network, and (2) the identification of known ransomware infections. The presence of a ransomware toolkit or infection indicates that an attacker has a foothold in the company's network and can successfully install ransomware on broader company infrastructure.

CyberCube can help brokers, carriers and reinsurers identify cyber risks on insureds' networks that are indicative of specific threats such as state-sponsored and criminal ransomware threats. CyberCube customers can identify specific companies or groups of companies that are susceptible to the tactics, techniques and procedures these particular threat actors use today. Identifying threat-specific risks at a single company or across a portfolio of companies can support proactive outreach to help prevent losses, and can help risk managers understand exposure and prepare to transfer risks related to top cyber threats.

THE SPECTRUM OF STATE SPONSORSHIP

It is important for cyber professionals to consider that the levels of relationship and, in particular, the nature of sponsorship between the various nation states and cyber criminals varies greatly. Some offensive cyber superpowers such as Russia, China, Iran and North Korea, have been known to provide a spectrum of support to cyber criminal actors as a means of incentivizing, growing and training cyber attackers who can be called on to do the bidding of that state. According to Jason Healey, senior fellow with the Cyber Statecraft Initiative at the Atlantic Council, the spectrum of nation-state support for cyber criminals can be categorized in the following way:

1. **STATE PROHIBITED** The national government has made cyber crime illegal and will prosecute criminals found guilty of transgression.

2. **STATE PROHIBITED BUT INADEQUATE ENFORCEMENT IN PLACE** The national government has made cyber crime illegal but is unable to enforce the associated laws.

3. **STATE IGNORED** The national government is unwilling to address cyber crime.

4. **STATE ENCOURAGED** Cyber criminals are encouraged by the national government as a matter of policy.

5. **STATE SHAPED** Cyber criminals are actively supported in their efforts by government resources.

6. **STATE COORDINATED** The national government coordinates criminal activity and influences operational detail.

7. **STATE ORDERED** The national government directs cyber criminals to conduct cyber attacks on its behalf.

8. **STATE ROGUE CONDUCTED** Certain government elements are involved in cyber attacks but this activity is not coordinated centrally.

9. **STATE EXECUTED** The national government conducts cyber attacks, with all associated elements under its direct control

10. **STATE INTEGRATED** The national government uses cyber attacks as a formal part of its strategic initiatives and uses both third parties and government resources in an integrated manner to conduct these attacks.

Future CyberCube reports on this topic will explore the spectrum of government sponsorship further, but it is important to consider that the range of support for criminal actors varies and that the situation is dynamic. The effective modeling of cyber events and the planned implementation of cyber defenses should take this spectrum into consideration. It is also important to consider that high levels of government support for cyber criminal actors, along with the proliferation of cyber weapons, have made it easier to move up the threat hierarchy.

Cyber professionals should consider that not all threat actors are equal, that criminals at the top of this hierarchy are the ones most likely to cause cyber events that are systemic in nature, and that these advanced actors often enjoy the support of national governments, both in terms of funding and of sponsorship and protection from legal proceedings. Currently, the strongest evidence of nation states and criminals working together involves the governments of North Korea, Russia and China. Known criminal actors, supported by these nation states can often be categorized as "Tier III and above" using the Threat Hierarchy shown in *Exhibit 2*.

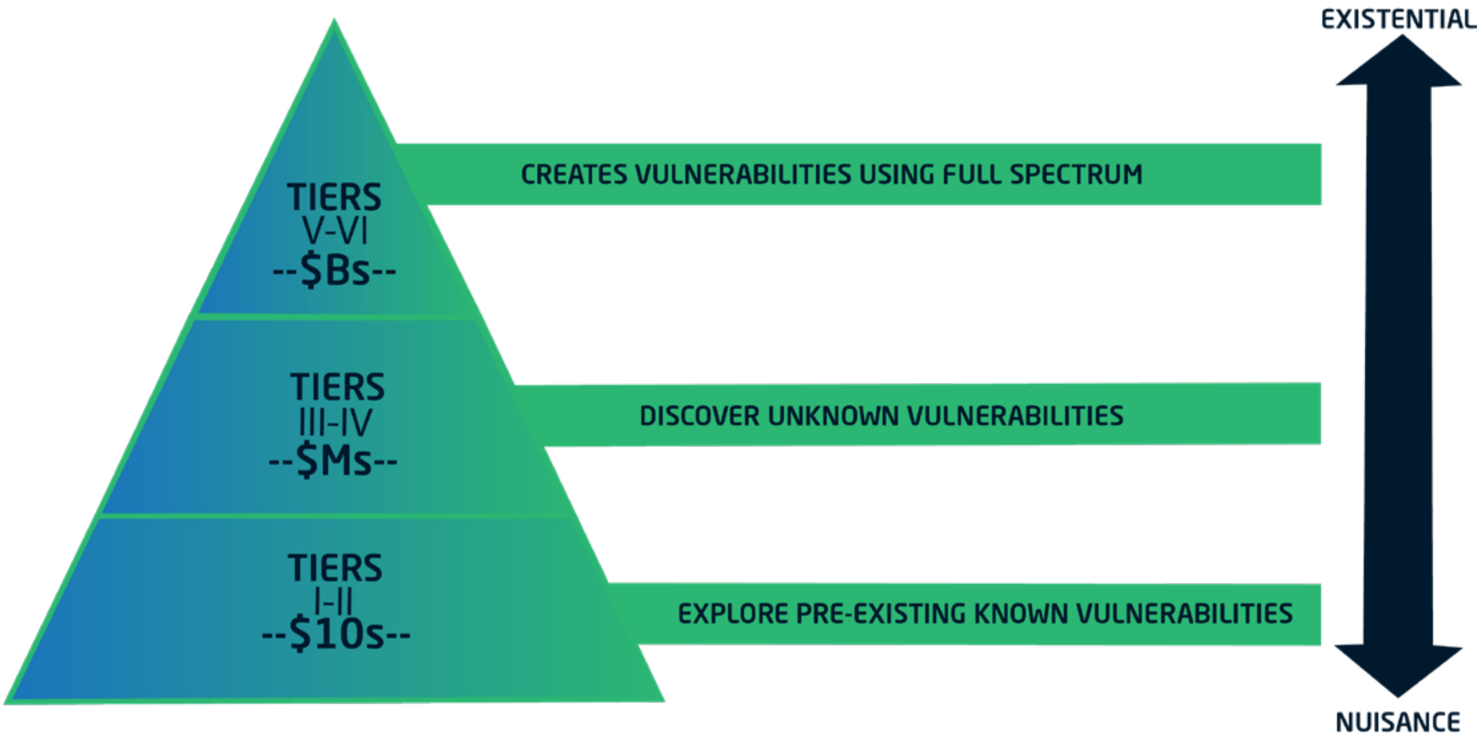

EXISTENTIAL
TIERS V-VI --$Bs--
CREATES VULNERABILITIES USING FULL SPECTRUM
TIERS III-IV --$Ms--
DISCOVER UNKNOWN VULNERABILITIES
TIERS I-II --$10s--
EXPLORE PRE-EXISTING KNOWN VULNERABILITIES
NUISANCE

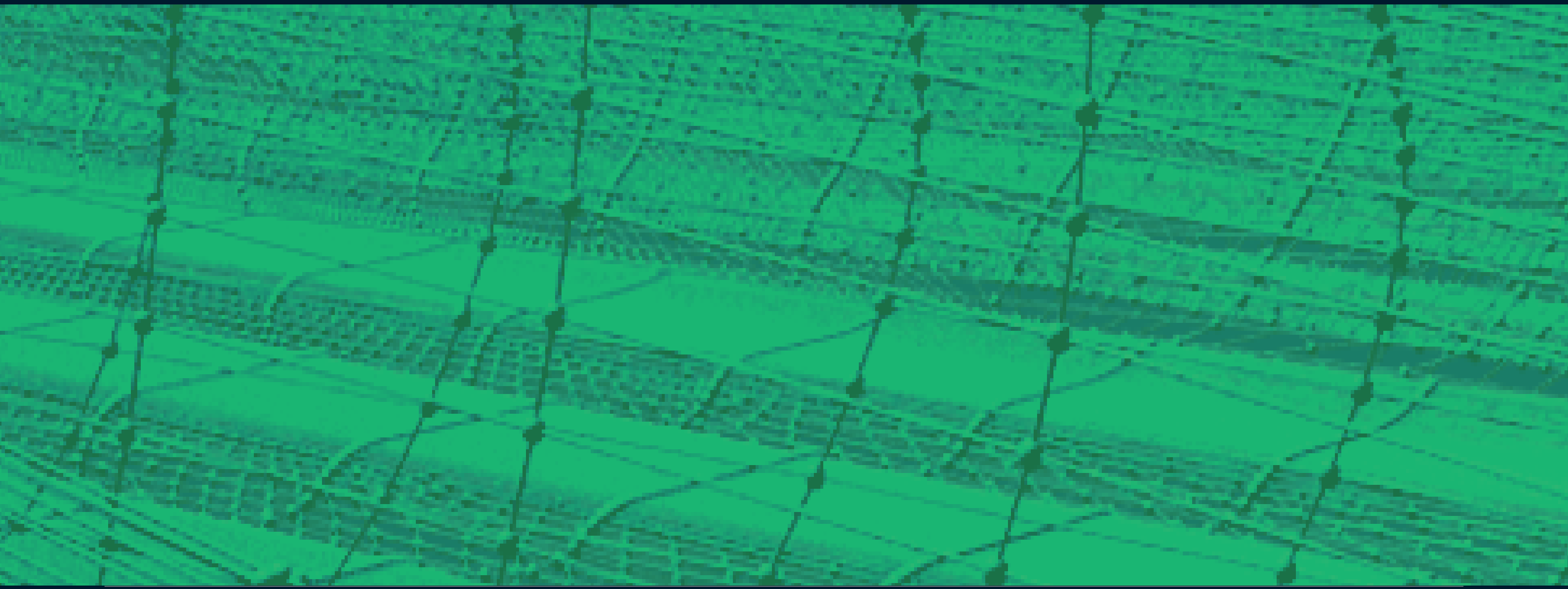
EXHIBIT 2

Cyber Threat Hierarchy (Source: US Dept. of Defense)

CONCLUSIONS

There is no shortage of documentation discussing the tactics, techniques and procedures used in modern cyber attacks, and cyber professionals, as well as insurers, should keep abreast of trends in this area. However, focusing entirely on these details, and not on the threat actors at play, is likely to lead to weaker cyber catastrophe modeling, underwriting practices, and cyber defense strategies.

Sun Tzu, author of The Art of War said, "If you know the enemy and know yourself, you need not fear the result of a hundred battles," and this philosophy holds true in the world of cyber warfare, cyber defense, and cyber insurance practices. The world of the threat actor is a complex one with a variety of motivations. Not all cyber criminals are built equally, and the cyber attacks we see every day come from actors whose competencies and maturities vary widely. Cyber risk professionals will be best prepared if they factor these elements into their cyber risk strategies.



AUTHORS:

Darren Thomson, Head of Cyber Intelligence Services
William Altman, Principal Cyber Security Consultant
Lea Hriciková, Cyber Security Consultant

EDITORIAL CONTENT:

Yvette Essen, Head of Content & Communications

DESIGN:

Alesia Auramenka, Graphic Designer

DISCLAIMER

For further information please contact:
CyberCube Analytics
58 Maiden Lane
3rd Floor
San Francisco CA94108
Email: info@cybcube.com
Telephone: +1(415)6354157

This document is for general information purpose only and is correct as at the date of publication. The product described in this document is distributed under separate licences with CyberCube which restricts its use, reproduction, distribution, decompilation and reverse engineering. Whilst all reasonable care has been taken in the preparation of this document including in ensuring the accuracy of its content, this document is provided on an "as is" basis and no liability is accepted by CyberCube and its affiliates for any loss or damage suffered as a result of reliance on any statement or opinion, or for any error or omission, or deficiency contained in the document. This document is subject to change from time to time and it is your responsibility for ensuring that you use the most updated version. This document and the information contained herein are CyberCube's confidential and proprietary information and may not be reproduced without CyberCube's prior written consent. Nothing herein shall be construed as conferring on you by implication or otherwise any licence or right to use CyberCube's intellectual property.All CyberCube's rights are reserved.

CyberCube is on a mission to deliver the world's leading cyber risk analytics.

We help the cyber insurance market grow profitably using our world-leading cyber risk analytics and products. The combined power of our unique data, multi-disciplinary analytics and cloud-based technology helps with insurance placement, underwriting selection and portfolio management and optimization. Our deep bench strength of experts from data science, security, threat intelligence, actuarial science, software engineering, and insurance helps the global insurance industry by selecting the best sources of data and curating it into datasets to identify trustworthy early indicators of risks and to build forward-looking views of them.

Discover how you can leverage leading cyber risk analytics for your busines
by contacting us at: sales@cybcube.com