GLOBAL GUARDIAN

# WORLDWIDE THREAT ASSESSMENT

**MAY 2022**

GLOBALGUARDIAN.COM 703.566.9463 INFO@GLOBALGUARDIAN.COM

TABLE OF CONTENTS





Global Guardian publishes an annual overview of recent global security developments. This year, Global Guardian's Intelligence Analysts have emphasized the digital threats that were accelerated and exacerbated by the COVID-19 pandemic. In addition, this report looks forward and assesses the post-pandemic world, where conflict over blood and soil is no longer a thing of the past. Ultimately, the goal of this report is to evaluate emerging risks and their impacts with a focus on how they will shape future safety and security concerns for global businesses and international travelers.

To meet these new challenges, Global Guardian offers an integrated suite of best-in-class security services that help clients identify and mitigate the risks associated with travel and conducting business both overseas and domestically. These services include personnel tracking, emergency response, security and transportation support, intelligence and due diligence, medical support and evacuation, emergency and custom aviation, cyber security, and video surveillance monitoring.

Global Guardian seamlessly integrates and delivers these capabilities 24-hours-a-day under the close guidance of its 24/7 Security Operations Center.

# END OF PAX AMERICANA?

**The war in Ukraine has thrust geopolitics back into the forefront of the world's consciousness. With American relative power in decline amid revanchist powers—including China, Russia, and Iran—possibly reaching their respective peaks, the era of relative peace that withstood the last 30 years may be now be ending.**

## INTERSTATE WAR—A THING OF THE PAST?

Russia's invasion of Ukraine marked the first time in more than 30 years that a country attempted to conquer its neighbor by force. By available metrics, conflicts have been becoming increasingly less deadly since World War II, largely due to fewer wars between states. Indeed, many thought that with the end of the Cold War, that inter-state war had, for the most part, been relegated to the past. This is because of Pax Americana—the era of relative peace, stability, and prosperity that extended throughout regions of American influence following WWII. It wasn't always this way. From 1816 to 1945, a state was subsumed, disappearing off the map, on average once every three years.

But since the end of the Cold War, America's relative strength and its willingness to use military, economic, and political might to uphold the norm against territorial conquest has been fundamental to preserving geopolitical stability.

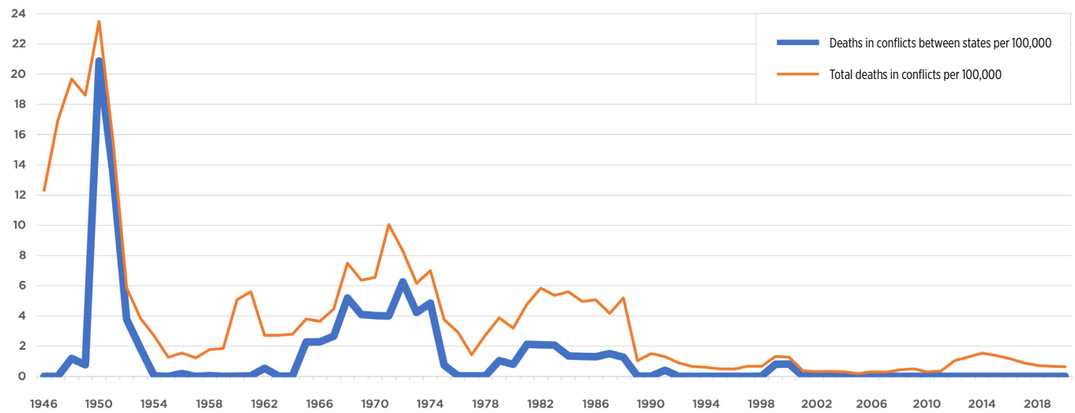
In no case was this more apparent than the response to Iraq's invasion of Kuwait in 1990. Through the auspices of the United Nations Security Council (UNSC), an American-led international coalition was authorized to repel Iraqi forces from Kuwait. The 1991 Gulf War was the zenith of the American-led international order, a time before other UNSC members, namely Russia and China, would use their veto powers for pure self interest at the expense of upholding international norms.

Today, there are growing signs that this era is over. Unlike in 1990, the international community is not united against the aggressing country. Due to the veto structure, there are no UNSC resolutions or global sanctions and while the West has coalesced to sanction and condemn Russia, the majority of the global population resides in countries that have stayed neutral.

Following Russia's invasion of Ukraine in February 2022, key Russian officials, Security Council Deputy Chairman Dmitry Medvedev and Foreign Minister Sergei Lavrov, framed the war as a battle to reshape the global order, proclaiming the end of the unipolar American moment. While at this early juncture, it does not appear that Russia will be fully successful in Ukraine, it is worth examining why President Putin decided that now was the opportune moment to reshape history.

**POST WWII DEATHS IN STATE-BASED CONFLICTS**

Civilian and military deaths in conflicts where the government of a state was a participant on at least one side




*Source: OWID based on UCDP/PRIO*

## TWILIGHT OF THE AMERICAN UNIPOLAR MOMENT

From the end of the Cold War until 2008, America's power was unbridled. But in the subsequent decade, U.S. relative power began to fade. Between the Great Recession, the legacy of the "Forever Wars" in Afghanistan and Iraq, and China's economic and military rise, America's relative position of dominance declined. Relatedly, societies in the West turned more inward. Not having been confronted by the prospects of major war in more than a generation and far enough removed from 9/11, voters became complacent towards foreign threats, unable to perceive the prospects of a return to inter-state conflicts.

Indeed, the first half of the story of American retrenchment is that of attrition. Despite their different styles of messaging, three consecutive administrations have remained consistent in this policy. The above-mentioned factors eroded the political will to use any force abroad, culminating in a series of events as displayed in the timeline below.

In parallel to the reluctance to use force, the over-reliance on economic sanctions as a tool of statecraft has become a theme. While the punitive economic effects of sanctions are profound, the efficacy of sanctions to deter bad behavior on their own—without the threat of force—has proven to be limited as seen through Russia, Syria, Iran, and North Korea's flagrant violations of norms. Due to China's increasing geoeconomic influence and China and Russia's permanent seats on the UNSC, U.S. and European sanctions have less of a deterrence value than they once did. Ultimately, there is a perception that America no longer has a preponderance of force to keep the peace and punish aggressors and norm breakers. This perception has been acted upon as seen by Russia's invasion of Ukraine.

The 2015 Iran nuclear deal and the current attempt to revive it are also illustrative of realization that it won't be politically viable for the U.S. to use military means

**THE EROSION OF AMERICAN DETERRENCE**

**2013**

**Syria Violates Chemical Weapons Red Line**

**Description:** In 2012, the U.S. establishes that the use of chemical weapons by Syrian forces would cross a "red line," prompting military intervention. When Syria does use sarin gas in August 2013, the U.S. does not intervene and instead, a U.S.—Russian negotiated deal to remove Syria's chemical weapons is brokered.

**Significance:** The lack of public support and political will in Washington to directly intervene demonstrated that after Afghanistan, Iraq, and—to an extent—Libya, that regime change had been removed from the foreign policy playbook.

**2014**

**Russian Annexation of Crimea & Support Rebels in Eastern Ukraine**

**Description:** Ununiformed Russian troops take over Crimea following the Euromaidan protests and subsequent revolution. Russia is expelled from the G8 and the U.S. sanctions President Putin's inner circle.

**Significance:** The U.S. and international community's tepid response to Russia's land grab portray weakness and signal an unwillingness to punish Russia for norm breaking.

**2019**

**Abqaiq Attacks**

**Description:** Iran and its proxies attack the worlds largest oil production facility in Saudi Arabia. The U.S. does not respond.

**Significance:**

1. The U.S. is not willing to enforce the Carter Doctrine (and "Reagan Corollary") which commit the U.S. to defending the production and export of Gulf oil.

2. Iran's cruise missiles and drones can evade U.S./Saudi defenses.

**2020**

**Mass Unrest & Contested U.S. Election**

**Description:** Over 10,000 protests are recorded with around 500 turning violent during the summer of 2020. The November presidential elections are contested, culminating with the storming of the Capitol on 06 January 2021.

**Significance:** From the outside, the U.S. appears highly distracted and internally divided—foreign policy leadership and strategic planning take a backseat.

**2021**

**U.S. Botches Afghanistan Withdrawal**

**Description:** The Taliban rapidly regains control of Afghanistan after the U.S. begins its withdrawal. Kabul is evacuated under Taliban control. A 26 August suicide bombing outside the Kabul airport kills an estimated 170 Afghans and 13 U.S. service members.

**Significance:**

1. American ability to reassure its partners is diminished.

2. Symbolic defeat of the most powerful military and political/logistic incompetence displayed.

to uphold the norm of nuclear non-proliferation. But not only is there a political constraint, a military one exists as well.

The second half of the story is that the proliferation of asymmetric technology, namely drones and missiles, now allows weaker actors to challenge American military primacy. During a House Armed Services Committee hearing in April 2021, General McKenzie, the commander of CENTCOM, lamented that for the first time since the Korean War, U.S. forces are operating without air superiority in Iraq and the Gulf. Iran's small and medium-sized armed drones, as well as its cruise missiles, can threaten U.S. forces at any time, challenging American dominance. A similar dynamic exists in the Pacific where China has developed an array of anti-access and area-denial (A2AD) capabilities, including its DF-21 and DF-26 anti-ship ballistic missile systems that can effectively endanger all aircraft carriers operating in theater.

Both Russia and Iran have repeatedly tested the United States (U.S.) directly or indirectly during these twilight years, but the question remains when—not if—China will follow suit?

### THE TAIWAN QUESTION

Russia has determined that now is its best opportunity, in part due to the new geopolitical realities, to reshape European security dynamics and rewrite the history of Ukraine. Like Russia, China may soon assess that the time is right to "reunify" with Taiwan—one of the regime's core interests. Just as Moscow seeks to change the status quo in Europe and assert sovereignty over a disputed area, Beijing desires to become Asia's preeminent power and change the status quo in disputed maritime areas. Another key, but underlooked, similarity between the cases of Russia and China is that while the window of opportunity for them may have been kicked open by the decline in American power, the window for action is actually closing for demographic and military reasons.

> "...while the window of opportunity for them may have been kicked open by the decline in American power, the window for action is actually closing for demographic and military reasons.

China is currently facing serious long term economic and demographic headwinds. With its slowed productivity growth and ballooning debt, China's investment-driven growth model is not sustainable. Bearish estimates show China's economic growth slowing to three percent a year by 2030. Meanwhile, China's population is growing at its slowest recorded pace as it ages. By 2040, a quarter of its population will be 60 or over. In effect, from now to 2050, China will swap 200 million working-aged adults for 200 million seniors. This process it about to accelerate over the next five years as China's labor force is set to start shrinking. So too will China's tax base. Its pension system may even run dry by 2035 without major intervention.

This comes at a time when its neighbors have increased their military spending and some have begun to band together in fora such as the Quadrilateral Security Dialogue (U.S., India, Japan, Australia) and AUKUS (Australia, United Kingdom, U.S.). It is no surprise that Asia and Oceania boasted the highest regional increase in spending in 2021. For the first time, even Europe has begun to perceive China as a strategic threat.

Enter Taiwan. Having witnessed Beijing annul its One Country Two Systems commitment to Hong Kong in 2020, it will almost certainly now never acquiesce to a peaceful reunification. Estimates from both Taiwan and the U.S. indicate that China may make its move before 2027 when it celebrates the 100th anniversary of the founding of China's People's Liberation Army (PLA). As it stands, the military balance is in China's favor. Simulating a Chinese invasion, Pentagon planners last year went 0-18 when defending Taiwan in different scenarios. Time is most certainly not on China's side, but it commands a sizeable advantage for now. While the fate of Taiwan may not be directly tied to that of Ukraine, the underlying global dynamics are the same and the the clock for China to seize Taiwan is ticking.

### TAKEAWAYS

The U.S. is evidently no longer the world's police—and revisionist powers have taken notice. The international system is in a state of limbo with the roles of its major players yet to be fully defined—somewhere between an American unipolar and truly multipolar world where regional powers compete and dominate their respective areas. The current danger lies in the transition where states see an opportunity and closing windows of action to reshape the map or regional power dynamics according to their preferences.



# DIGITAL PICKPOCKETS: HACKERS TARGET CRYPTOCURRENCY EXCHANGES

**Cryptocurrencies (crypto) surged in value in 2021 as people flocked to invest stimulus cash using simplified cryptocurrency exchange services. A lack of consumer protections and crypto's high value have led hackers to focus on crypto exchanges as low-risk, high-reward targets—leaving victims with empty wallets and no way to recover lost funds.**

### A DIGITAL FUTURE

In 2021, cryptocurrency became mainstream as market penetration among U.S. consumers reached an all-time high. Crypto's meteoric rise coincided with the transition to work-from-home employment and the provision of thousands of dollars in COVID-19 stimulus payments. These factors, together with bitcoin's history of rapid investment returns since 2017 have encouraged more people to trade crypto on virtual exchange sites, including Coinbase. Operating like stock exchanges for cryptocurrencies, crypto exchanges have followed bitcoin's rise. By establishing networks with major banks, crypto exchanges have attracted new investors by making crypto purchasing easy and accessible to those without any technical knowledge of cryptocurrency. Today, consumer interest continues to grow as crypto exchanges ramp up marketing efforts, with several exchanges competing for prime-time Super Bowl ads.

### HIGH STAKES

Cryptocurrency's lucrative rise has given hackers more opportunity and incentive than ever to target retail investors. More consumers exchanging more money with crypto has made crypto investors irresistibly high-value targets for hackers. With a lack of mandatory cyber security standards and cybercrime's low barrier to entry, cryptocurrency theft has become profitable, low-risk, and increasingly frequent.

In addition, the expansion of international crypto mining enterprises has made it more difficult for the average tech-savvy cryptocurrency miner to make money. Crypto mining allows anyone to obtain crypto without purchasing it directly by building specialized computers to run crypto mining software. These computers solve thousands of complex mathematical problems per second while trying to guess a secret, random number that will reward the builder with cryptocurrency.

Crypto mining is therefore designed to reward the person with the most computer processing power. As competition to obtain crypto has increased alongside its value, entire organizations now specialize in crypto mining. Today, the soaring costs of high-performance graphics cards have made mining prohibitively expensive at the scale required to compete. The crypto mining process itself is also power intensive, further raising the financial barrier to entry for the average person due to the energy costs.

By expending more money and energy to mine cryptocurrency than anyone else, massive crypto mining enterprises have all but eliminated the ability of hobbyist crypto miners to compete. As a result, would-be crypto miners have lost an incentive to compete fairly, while the incentive to invest in skills to obtain crypto via illicit means has been amplified by crypto's high value.

It is, therefore, no surprise that 2021 was the most rewarding year for crypto thieves, with heists amounting to USD $14 billion. The cost is expected to rise in 2022, as hackers continue to target crypto exchanges by exploiting vulnerabilities between the exchange's web platform and software, called wallets. Wallets are provided by crypto exchanges for people to securely buy, sell, and store private

access to their cryptocurrency. Unauthorized withdrawals from crypto wallets are the primary means exploited by hackers to steal cryptocurrency. As the stakes have risen to find new ways into wallets, hackers have developed new vectors that now have crypto exchanges on the defensive.

## HIDDEN VULNERABILITIES

In the most damaging attacks, hackers hijack communications between the crypto exchange platform's internal network and private accounts using stolen access credentials. These are known as Man-in-the-Middle (MITM) attacks. Hackers commonly steal these credentials through a supply chain attack using a third-party software-as-a-service (SaaS) application. The SaaS app might help the crypto exchange manage data, support messaging or email, or enable employees to access servers remotely. This is one explanation for the recent Crypto.com hack that cost the company over USD $34 million in January 2022 and required Crypto.com to reset Two-Factor Authentication (2FA) tokens for all accounts (see box for details).

If a hacker can inject code into a third-party SaaS program update through a code exploit or successful phishing attempt, the SaaS program can infect client networks like Crypto.com with malware that gives the hacker access to the client's internal systems. Once inside, hackers gain access to the sections of the internal network serviced by the SaaS app and exploit network traffic to laterally move beyond this access point. If hackers can connect to an external command and control server (C&C) through misconfigured or compromised security controls, they can steal files, profile systems, and upload further malware, setting up a MITM attack—all without leaving much of a trace.

From a MITM, hackers can continuously monitor network traffic and launch enterprise-level Pass-The-Cookie (PTC) attacks. A PTC attack collects session cookies, which are generated by an authentication server and sent to a person's computer after they log in. A PTC attack exploits cookie authentication to bypass security controls, including passwords and 2FA. Since session cookies operate like a pass into a restricted area, hackers can use a captured cookie as a direct line into accounts by injecting it into their own browsing session if cookie permissions are not set to expire quickly enough.

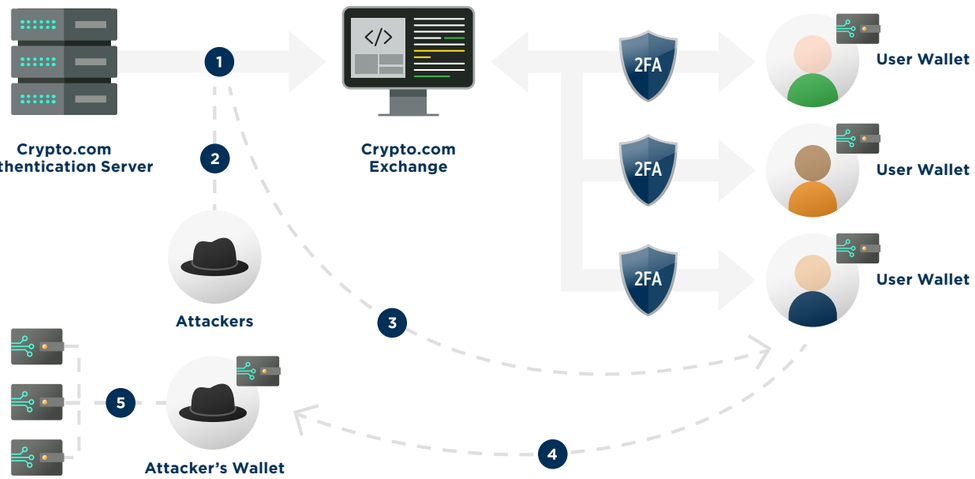
In such a scenario, unauthorized transactions would flow from exchange wallets to an attacker's non-exchange wallet without the owner receiving notifications of a security breach. Further, existing 2FA controls would be ineffective and even vulnerable to exploitation without knowing what information the hacker managed to extract. This result matches the security measures enacted with Crypto.com's response to the January 2022 cyber incident.

Victims affected by the Crypto.com hack and other attacks on crypto exchanges have no legal recourse or way to retrieve lost funds. Although victims can see where the crypto was transferred to on the public ledger, hackers use services called crypto mixers to split stolen funds across hundreds of wallets to hide their origin. Even if the stolen crypto is located, it cannot be taken back unless the attacker's private key is used to transfer it. The most that victims can hope for is support from the crypto exchange itself, which may or may not choose to issue credit.

To avoid becoming a victim of crypto thieves, the best protection crypto investors have while on the exchange is to take action to go beyond 2FA or other circumventable software access controls.

### CASE STUDY: CRYPTO.COM HACK

Around midnight on 17 January 2022, USD $34.65 million of Bitcoin and Ethereum disappeared in an instant as 483 Crypto.com users had unauthorized persons drain their cryptocurrency accounts of funds. Despite enabling mandatory 2FA, users were not made aware of the theft until logging on the next day.




#### STAGES OF A CRYPTO EXCHANGE HACK

1. Server authenticates user credentials to access Crypto.com.
2. Attackers intercept Crypto.com's internal server traffic.
3. Attackers bypass user 2-Factor Authentication access controls by hijacking communication between the authentication server and the exchange.
4. Funds are drained from user wallets to the attacker's wallet without warning.
5. Stolen funds were split and transferred using crypto mixing service Tornado Cash, masking their origin and complicating recovery.

The wallet keeps a running balance of how much crypto is tied to it through these keys. Wallets provided by exchanges help by remembering passwords which simplifies transactions for investors. Most hacks targeting crypto exchanges from within seek to gain access to the wallet for this reason. With the private key, hackers can transfer the victim's cryptocurrency freely.

> One way to prevent this from happening is to hold money offline on a "cold" wallet—one that is not connected to a crypto exchange. While one will need to move the funds from a "cold" to a "hot" wallet—one that is online and linked to an exchange—for the purpose of transaction, funds can then be subsequently moved back to the "cold" wallet upon completion.

One way to prevent this from happening is to hold money offline on a "cold" wallet—one that is not connected to a crypto exchange. While one would need to move the funds from a "cold" to a "hot" wallet—one that is online and linked to an exchange—for the purpose of transaction, funds can then be subsequently moved back to the "cold" wallet upon completion. Diversification is another strategy to mitigate the risk of losing cryptocurrency to cybertheft. Maintaining accounts ("hot" wallets) on multiple crypto exchanges can dampen the blow should one exchange become compromised.

## THREAT MITIGATION

To understand how to protect a crypto wallet, it helps to understand what makes it different from a traditional wallet. Instead of money, a crypto wallet holds complex passwords to access and transfer crypto called public and private keys. The public key is used to receive crypto for payments, while the private key is for spending.

## TAKEAWAYS

Crypto exchanges are persistently exploited by hackers to steal cryptocurrency because of crypto's reputation as a high-value, low-risk target. Crypto investors should go beyond Two-Factor Authentication by taking crypto assets off the exchange and into offline wallets when not in use.

# RANSOMWARE IN 2022: DOWN BUT NOT OUT

**Despite the unprecedented successes of law enforcement against cybercriminal groups in 2021, the threat of ransomware remains critical. The most sophisticated groups have evolved and are poised to cause major problems for organizations in the coming year by exploiting new vulnerabilities and taking advantage of the geopolitical environment to maximally extort their victims.**

## 2021 IN REVIEW

The year 2021 featured several high-profile ransomware attacks, including when DarkSide took Colonial Pipeline hostage in May 2021, instigating panic and supply shortages. However, 2021 also saw an unprecedented uptick in law enforcement operations against ransomware collectives.

Several weeks after the Colonial Pipeline attack, DarkSide's infrastructure and cryptocurrency profits—approximately USD $4 million in Bitcoin—were seized by law enforcement. In addition, authorities blocked DarkSide's hosting panels, payment servers, and blog, leaving the group toothless. REvil, the ransomware group that attacked JBS meat distributors and Kaseya management software in the summer of 2021, was shut down after a multinational law enforcement operation. Romanian and South Korean police arrested five people associated with REvil and U.S. officials issued indictments against a Ukrainian national and a Russian national for involvement with the group. Law enforcement further seized over USD $6 million in cryptocurrency from the group.

DarkSide attempted to reemerge under a new name, BlackMatter, but again, it was shut down due to law enforcement pressure.

## MORE MONEY, MORE PROBLEMS

Last year's gains against ransomware groups do not necessarily envisage another year of successes for law enforcement. As officials moved to shut down ransomware operations after high-profile attacks, cybercriminals have adapted to targeting mid-sized organizations. While mid-sized companies may not offer up the largest ransom sums, they often have weaker cyber security protocols than large enterprises, and attacks on them draw less law enforcement attention. The costs of recovery from a ransomware attack more than doubled in 2021. The average total cost for a firm recovering from a ransomware attack rose to over USD $1.85 million in 2021, up from USD $761,106 in 2020. This figure includes downtime, lost orders, operational costs, and ransom payments to threat actors. The ransom payments firms made to ransomware groups in order to recover their data rose exponentially over the past two years, hitting an average of USD $170,404, up from USD $41,198 in 2019.

All this spells trouble for enterprises lured into a false sense of security by government announcements and high-profile ransomware group shutdowns. Ransomware remains a major cyber security concern for organizations, and the threat is poised to continue.

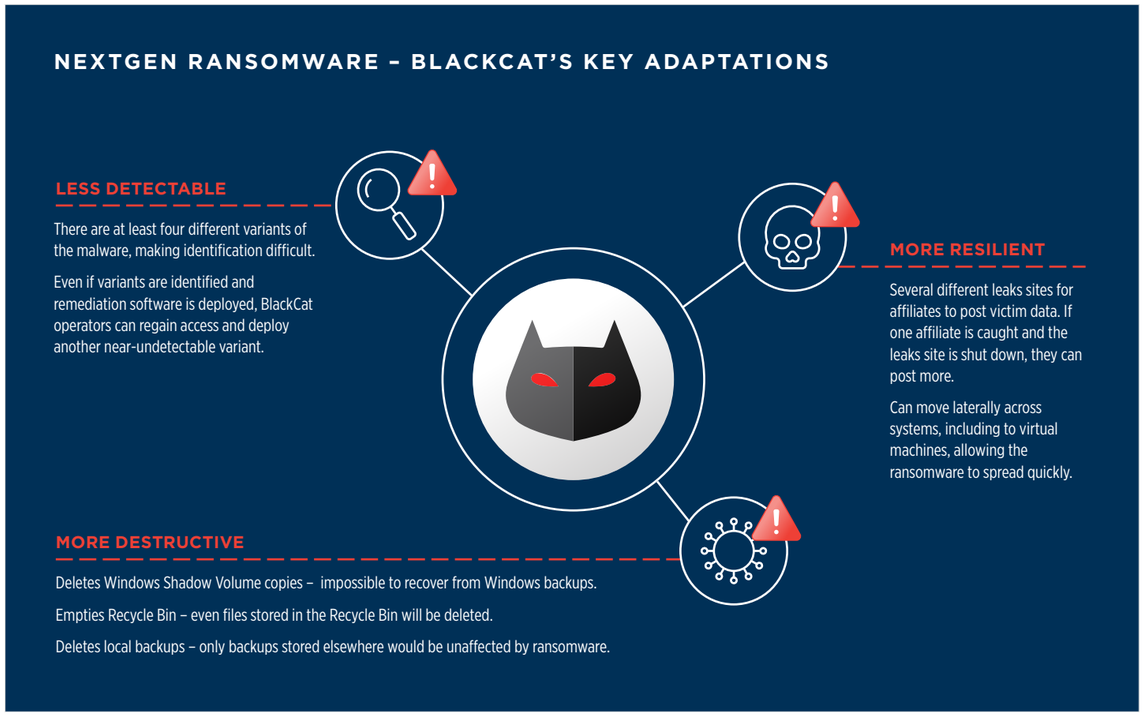
## WHAT COMES NEXT?

Today, there are three main factors that will contribute to the continued proliferation and success of ransomware groups. First, ransomware gangs have shown an ability to adapt their tactics, techniques, and procedures (TTPs) and evolve in an increasingly hostile environment. Second, new, recently exposed vulnerabilities—like the Log4j vulnerability—allow ransomware groups dangerous vectors to carry out their attacks. Finally, geopolitical tensions could erase the leaps in combating ransomware and allow nefarious groups to prosper in safe havens.

1. **Adaptation:** Emerging ransomware groups have adapted to the new hostile environment and have changed their TTPs to make themselves less detectable, more resilient, and more destructive. November 2021 saw the emergence of BlackCat ransomware group (also known as ALPHV), which some researchers claim is a successor to DarkSide and REvil. Notably, the BlackCat software is the first ransomware to be written in Rust, a high-performance programming language, which offers coders memory safety, allowing them to be protected from software bugs when encrypting a victim's system. BlackCat's Rust-based malware facilitates its operational security, while adding no extra overhead runtime for executing the program, allowing the ransomware to complete complex encryption before victims have the chance to notice that they have been impacted. The group has already claimed several high-profile victims in the construction and engineering, retail, transportation, commercial services, insurance, machinery, professional services, telecommunication, auto components, and pharmaceuticals industries, and is advertising itself to fellow threat actors as "the next generation of ransomware" (see box on opposite page).

2. **Exposed Vulnerabilities:** The discovery of the new and dangerous Log4j vulnerability in December 2021 will further act as a boon to ransomware groups. Log4j, one of the most serious vulnerabilities in decades, is a software used to record computer activities in popular games as games, such as Minecraft, and cloud services, including Amazon Web Services. Ransomware groups have already begun weaponizing the vulnerability and using it to gain access to exposed virtual machine centers, which organizations use to connect employee machines to organizational servers, even when the employee is working remotely. In December 2021, members of the Conti ransomware group, one of the most active ransomware groups of 2021, used the Log4j vulnerability as an initial attack vector against a victim. It moved laterally across the victims' network after first infecting a single machine. The Conti group used Log4j to gain access to and encrypt virtual machines on an organizational network. While an updated patch for the vulnerability has been released to the public, it is only useful if it has been downloaded. Log4j will be a windfall to enterprising ransomware groups.

3. **Geopolitical Tensions:** Strained Russo-Western relations in 2022 will erase the progress made towards combating ransomware. Most ransomware groups find safe harbor in Russia, where the government does not prosecute ransomware operators, in exchange for a tacit promise not to attack Russian institutions. After REvil's shutdown, many suspected that Russia was involved in the takedown operation after pressure was exerted by President Biden. As tensions between Russia and the West reach unprecedented heights, the risk of ransomware attacks out of Russia increases. It is possible that Russia will give even greater free reign to ransomware groups within its borders and overlook even the most egregious attacks. Additionally, advanced persistent threat (APT) groups linked to the Russian state could deploy ransomware against US-based institutions as additional pressure to leverage as it confronts the U.S. and NATO.




## TAKEAWAYS

Ransomware groups might have been bruised in 2021 but they have not been defeated. New innovations, vulnerabilities, and geopolitical tensions point to more complex and persistent ransomware attacks. This poses a real danger to organizations, as ransomware attacks have become more damaging to a business' bottom line and reputation.

# 3D PRINTING: THE DIY ARMS REVOLUTION

**3D printed weapons are now starting to reach maturity. While 3D printed arms do not currently constitute a major threat in the U.S., they do in Europe, Asia and Australasia. Today, 3D printing has reached the point in its development where reliable and untraceable weapons are easy enough to make that a motivated, average person with no technological expertise can build a reliable gun at home for around USD $500, with subsequent units only costing USD $100. What began as an expression of freedom and as a check on real or perceived tyranny, is now showing its first signs of being coopted by extremists and criminals. As 3D printing technology continues to advance and become more accessible, malicious actors—from extremists to gang members—will be able to acquire increasingly lethal and reliable weapons.**

## 3D PRINTED GUNS TODAY

3D printed guns have been around for almost a decade, yet only recently have they reached widescale adoption. In October 2019, a White supremacist attempted an attack on a synagogue in Halle, a town in eastern Germany. The assailant used home-made weapons which included improvised guns made partially from 3D printed parts, marking the first documented instance of 3D printed weapons being used by an extremist. The attack failed when the assailant couldn't gain access to the synagogue and his improvised weapons repeatedly jammed, but he was able to kill one individual in a nearby kebab shop.

Just a few months later, in 2020, designs for the FGC-9 carbine were unveiled and disseminated by Deterrence Dispensed, a decentralized and global peer-to-peer community of 3D gun enthusiasts. Unlike previous models of 3D printed guns, the FGC-9 can be built solely from unregulated parts without specialized tooling or expertise in gun making. It can be assembled with around 80 percent 3D printed parts (almost everything but the barrel can be printed). Even the parts that cannot be printed can be made with the help of tools that can be 3D printed, highlighting the productive power of 3D printing to the at-home gunsmith. While there is no verifiable data surrounding the efficacy and durability of the FGC-9, per accounts, it is fairly dependable, accurate at short distances, and can fire several thousand rounds before starting to break down.

Indeed, images of the FGC-9 began to emerge from Myanmar in December 2021, marking its first combat use. It is rumored that the People's Defence Forces (PDF), the armed branch of the elected National Unity Government uses the FGC-9. The PDF can inexpensively print and machine the requisite parts as needed and has been using the weapons for close distance raids on the Tatmadaw (the military junta's forces). Meanwhile, the FGC-9 has been found by police in gang raids in the UK, Spain, and New Zealand; and was recently spotted in photos from the Irish Republican group Óglaigh na hÉireann (ONH) in a threatening Easter address.

### EVOLUTION OF 3D PRINTED WEAPONS

**1987** First 3D Printing Machine Built

**2013** First 3D Printed Pistol (The Liberator) Unveiled by Defense Distributed

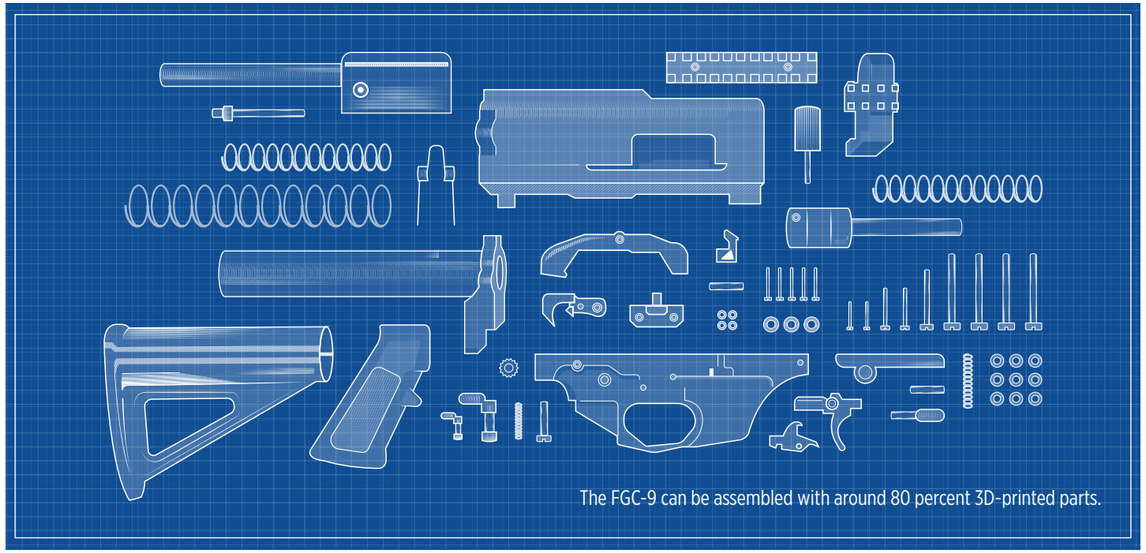
**2019** Halle, Germany Shooting – 3D Printed Weapons Fail

**2020** Reliable and Easy to Make 3D Printed Carbine (FGC-9) Unveiled by Deterrence Dispensed

**2021** FGC-9 Used in Myanmar Civil War

## THE THREAT

In the U.S., it is and will continue to be easier to purchase a firearm legally or illegally than to 3D print them—malicious actors will always seek the path of least resistance. Though 3D printed weapons could benefit extremists and extremist groups who wish to maintain a low profile and not risk exposure to law enforcement by buying weapons or weapon parts in ways that can be traced. While 3D printed guns pose little additional threat in the U.S. where legal and illegal firearms are ubiquitous and easy to acquire, 3D printed weapons have the potential to upset the balance of force between criminal enterprises and increase the lethality of future terrorist attacks in Europe from both Islamic extremists and White nationalists. Being able to manufacture your own weapons gives lone wolves, smaller street gangs, or even decentralized terror cells the ability to punch above their weight. In the criminal underworld, any change to power relations results in bloodshed, often with collateral damage.




*Graphic for illustrative purposes only.*

## BY 2030

Currently, an individual does need to be highly motivated to create their own 3D printed weapons in a process that can take weeks. However, as the online community grows, and technology advances, the ability to make weapons—not just rifles, pistols, and carbines, but even explosives—will become much easier. Moreover, the 3D weapons themselves will soon match the quality of their factory-produced counterparts.

Much like the 3D printing industry writ large, the cost of 3D printing metal has rapidly declined. Today, a printer capable of making metal parts costs around USD $100,000. While this is still cost prohibitive, the cost of metal printing systems will continue to decrease, as will the build times and the effort needed to produce firearms. Similarly, as more and more small- to medium-sized manufactures adopt 3D printing and offer to fabricate designs from digital files provided by their customers, nefarious actors could leverage these manufacturers to professionally produce the more complicated components. But the proliferation of guns made in basements isn't the only threat in the medium term.

Just as gun design files have evolved over the last decade and an anonymous internet community has coalesced around the idea of making it as easy as possible to create DIY firearms, it is probable that over the next decade, this community will begin to share other forms of 3D printed weaponry. Both the U.S. Department of Defense and UK Ministry of Defence are experimenting with 3D printed explosives that can be fabricated on location in combat zones. With the advent of multi-material 3D printing, it is already possible to fabricate explosives from constituent materials, which are widely available and would not raise concern until they are combined. So long as the internet remains open and retail 3D printers are allowed to be sold, the production of progressively more effective, easy to make, and inexpensive DIY weapons will continue.

### TAKEAWAYS

In the near term, 3D-printed weapons bolster the lethality of lone wolf extremists, especially in countries with heavily restricted access to firearms. From the ability to quickly and economically produce high quality weaponry and ammunition to the ability to manufacture explosives, over the coming decade, 3D printing technology will have the potential to revolutionize the social contract between government and the people, challenging the government's monopoly on violence.

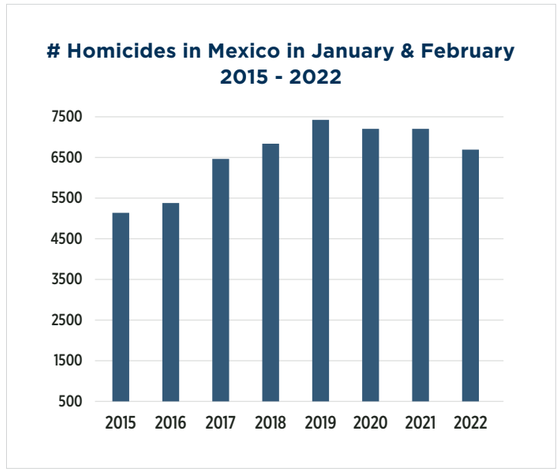
# COVID-19 AND THE GLOBAL CRIME WAVE


**Countries are ending pandemic restrictions against a backdrop of high violent crime rates. Often propelled by country-specific factors, in addition to economic distress and general uncertainty, it will be long before crime rates return to pre-pandemic levels in many countries.**

In 2022, national crime trends show no sign of reverting to their pre-pandemic trajectories. As the world opens up and travel resumes, opportunities for theft, robbery, drug smuggling, and kidnapping are rebounding globally. While the uptick in crime is not universal within any region, it is manifesting across different geographies in different ways—some more violent than others.

## MEXICO

No Latin American country demonstrates a sustained rise in violent crime more clearly than Mexico, where homicides have soared roughly 30 percent since 2015. Despite a modest drop of seven percent in 2022, Mexico's overall homicide rate has remained at historically high levels, hovering between 26 and 29 murders per 100,000 citizens. Armed robberies, kidnappings, and carjackings by drug cartels are driving the upward trend in violent crime throughout Mexico, with some of the highest rates observed in the first few months of 2022 in Baja California, Jalisco, Puebla, and Mexico City, as cartel battles and murders of police and journalists have reached a fever pitch. The high mortality of police officers and reorganization of Mexico's criminal justice system over the past few years have, in turn, led to fewer investigations and fewer arrests, leaving civilians without any recourse except to seek justice on their own. This lack of effective law enforcement amid budgetary strain that predates COVID-19 has caused Mexico's internal security situation to suffer from severe systemic issues that are unlikely to be solved any time soon.




*Source: ELCRI*

## UNITED STATES

In the U.S., murders rose by 30 percent in 2020, followed by a five percent increase in 2021. Meanwhile, arrests plummeted 24 percent—the lowest number in 25 years, according to FBI data. Although the pace of violent crime, including murder, slowed in 2021, four U.S. cities—including Portland, Austin, Rochester, and Philadelphia—reported breaking records for the most annual homicides since the 1990s. On the criminal justice side, prisoners that were released early to avert the spread of the virus and violent offenders released on zero-bail policies faced high rates of recidivism, while police began to face a crisis of confidence from the public that continues to limit the effectiveness of law enforcement. Together, these factors caused a jump in robbery, murder, and assault. As the U.S. economy returns to normal operations, the lingering momentum of these trends suggest that a reversal to pre-pandemic levels will be slower than the initial rise of violence in 2020.


*Source: ABC News*

## NIGERIA

Nigeria, home to an extensive criminal network, has been one of the countries most affected by the crime wave following COVID-19. Organized criminal activity flourished across West Africa during the pandemic as economic devastation pushed people to turn to the drug trade for alternative sources of income. At the same time, travel restrictions halted drug and migrant smuggling operations that financed Nigeria's organized crime groups. These groups, ranging from local gangs to armed militant organizations—including Boko Haram and the Islamic State—in West Africa, subsequently expanded their operations in kidnapping for ransom, armed robbery, and extortion to make up for the loss in profits. Between 2019 and 2020, the number of kidnapping victims in Nigeria increased by 51 percent as criminal organizations abducted train passengers and schoolchildren by the dozens. Parts of Nigeria in the north and south have become ungovernable due to brazen attacks by these militant groups. This trend is unlikely to reverse course in the short term while kidnapping for ransom remains efficient and profitable.

## INDIA

At first glance, crime in India is on the decline. In the context of India's COVID-19 lockdown from 25 March to 31 May 2020, property crimes, including burglary and theft, decreased by 24 percent. In 2020, India likewise saw kidnappings fall by 19 percent alongside an almost three percent decrease in murders. This caused India's murder rate to plateau at roughly two incidents per 100,000 population. However, during this same period, violent crime against scheduled caste and tribe members—some of India's most marginalized groups—increased by nine percent nationwide. After 2020's temporary decline, attempted murders jumped by 35 percent in India's capital city of Delhi while incidents of extortion and kidnapping each ballooned by nearly 50 percent. Together, these trends suggest violent crime trends in India may be worse than the currently available data indicates.

## SWEDEN

Outside of violent crimes committed by Sweden's gangs, other crime, including non-violent property crimes, fraud, and theft, declined during the pandemic and continue to trend downward even as lockdowns have been lifted. However, following a rise in gang activity between 2015 and 2020, Sweden's homicide rate rose 38 percent and has since remained at its highest level since the early 2000s. Sweden has become notorious as home to Malmö and Göteborg—some of Europe's most dangerous cities—where gangs wage turf wars for control over the Swedish drug trade. The frequency of gang shootings alone caused the nation's rate of gun homicides to jump to 4.5 times the European average. Sweden's gang violence has also been marked by a rising trend in bombings using homemade devices, or IEDs, which became deadly apparent in September 2021, when a bomb went off in an apartment building in Göteborg, injuring 16 people. The lack of evidence left behind by detonated IEDs has complicated Swedish officials' abilities to crack down on the violence, which has persisted despite Sweden's overall low crime rate and Swedish authorities' efforts.

## TAKEAWAYS

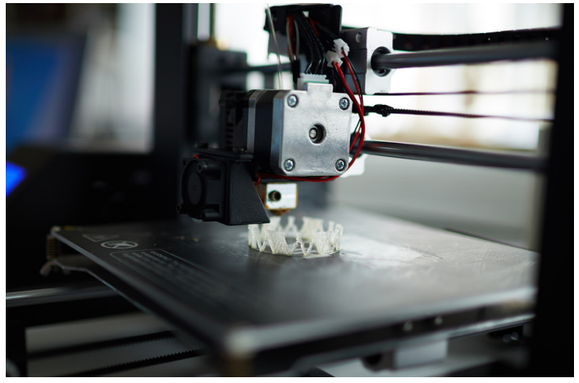
Violent crime trends—from homicide to kidnappings, assault, and robbery—have changed trajectory within most regions of the world since the start of the COVID-19 pandemic in 2020. Violent and non-violent crime rates are unlikely to return to pre-pandemic levels within the next few years, especially within underdeveloped nations where the institutions and rule of law are weak and the economic recovery will be slow.

# OUTLOOK AND TAKEAWAYS

**On the heels of a once-in-a-hundred-year global pandemic, the world is now in the midst of its first largescale interstate war involving a major power in over 30 years. These extreme events that were previously thought to have been things of the past have returned with a vengeance. The clustering of such events speaks to the covariate nature of risk in today's world. From geopolitics to the digital realm, the COVID-19 pandemic has ushered in an era of uncertainty where bad actors at both the state and substate levels are taking advantage.**

## GEOPOLITICS

On the international stage, Russian leaders are seizing on the pandemic-driven state of flux. Following America's ill-executed exit from Afghanistan, revanchist powers—including China, Russia, and Iran—are no longer deterred and see now as the opportune moment to reshape the map and regional security dynamics before its too late. The relative peace and stability that American hegemony fostered after World War II, and especially in the post-Cold War period, is very much in question. While the norm of territorial conquest is being broken now, the current geopolitical environment is opening the door to nuclear proliferation being the next major norm to be broken. In addition, in this new power void, regional powers will compete and dominate their respective areas.



## TECHNOLOGY

In December 2021, pictures of 3D printed weapons from Myanmar's civil war began to surface, marking the first time that these DIY weapons have been used in combat. Now having reached maturity, these 3D printed weapons will make it easier for malicious actors—from extremists to gang members—to acquire increasingly lethal and reliable weapons. While the threat these weapons pose in the U.S. is still quite limited in the near term, 3D printed weapons will be able to challenge the government's monopoly on violence in the long run, especially in countries with heavily restricted access to firearms.

## CYBER

The remote working revolution and economic realities that were spurred by the pandemic accelerated the pace at which cybercrime has afflicted businesses and individuals. Despite unprecedented law enforcement action against cybercriminal groups in 2021, new innovations, vulnerabilities, and geopolitical tensions portend more complex and persistent ransomware attacks. In a similar vein, the January 2022 Crypto.com hack, in which over USD $34 million of Bitcoin and Ethereum were stolen, highlights the sophistication of highly motivated cybercriminals. In what was likely a supply chain hack, criminals were eventually able to circumvent industry standard software access controls to steal users' money, leaving the victims without legal recourse. Crypto investors should go beyond Two-Factor Authentication by taking crypto assets off the exchange and into offline wallets when not in use.

## CRIME

The uptick in crime linked to the COVID-19 pandemic is manifesting across different geographies in different ways—some more violent than others. While there are country-specific factors at play, such as the socio-political environment in the U.S., economic distress and general uncertainty were universal contributing factors. Violent and non-violent crime rates are unlikely to return to pre-pandemic levels within the next few years, especially in underdeveloped nations where the rule of law is weak and the economic recovery is projected to be slow.

## ABOUT GLOBAL GUARDIAN

Global Guardian is a leading duty of care firm that provides corporate, government, and family clients with real outcomes to a range of security and medical incidents and emergencies. Our comprehensive suite of innovative solutions—including real-time monitoring and location awareness technology, emergency response and evacuations, medical support and transportation, and global intelligence—are available at the push of a button and backed by our U.S.-based 24/7/365 Security Operations Centers and local response teams in over 130 countries.

## GLOBAL INTELLIGENCE

Our team is standing by to support when global events have the potential to impact your organization, people, and operations. Global Guardian's intelligence analysts know the localized nuances and threats in regions throughout the world and can provide in-depth custom reports for clients and organizations in need of daily, weekly, or monthly real-time intelligence and analysis of events. To learn more about our intelligence products or start building your own custom report, email intelligence@globalguardian.com.

**Global Guardian**
8280 Greensboro Dr. Suite 750
McLean, VA 22102, United States

**Global Guardian London**
99 Bishopsgate
London EC2M 3XD, United Kingdom

**Global Guardian Asset Security**
2127 Ayrsley Town Blvd. Suite 201
Charlotte, NC 28273, United States

+1.703.566.9463
info@globalguardian.com
globalguardian.com