Security Now! #861 - 03-08-22

Rogue Nation Cyber Consequences

This week on Security Now!

This week we examine many of the cyber-consequences of Russia's unilateral aggression against Ukraine. In a world as interconnected as today, can a rogue nation go it alone? Ukraine has formed a volunteer IT Army, hacking groups are picking sides, is StarLink a hope? Actors on both sides of Russia's borders are selectively blocking Internet content, Google has become proactive, the Namecheap registrar has withdrawn service, use of the Telegram encrpyted messenger service as exploded, crypto currency exchanges block 10's of thousands of wallets, Russia releases the IP addresses and domains attacking them (and likely some which are not), they also prepare to amend their laws to permit software piracy and appear to be preparing to entirely disconnect from the global Internet. All of the technologies we've been talking about for years are in play.

"Of course this website is safe. As an extra measure of security, they make you sign in with your Social Security number, mother's name, your bank account, home address, phone number and date of birth."

Security News

The Russians are coming

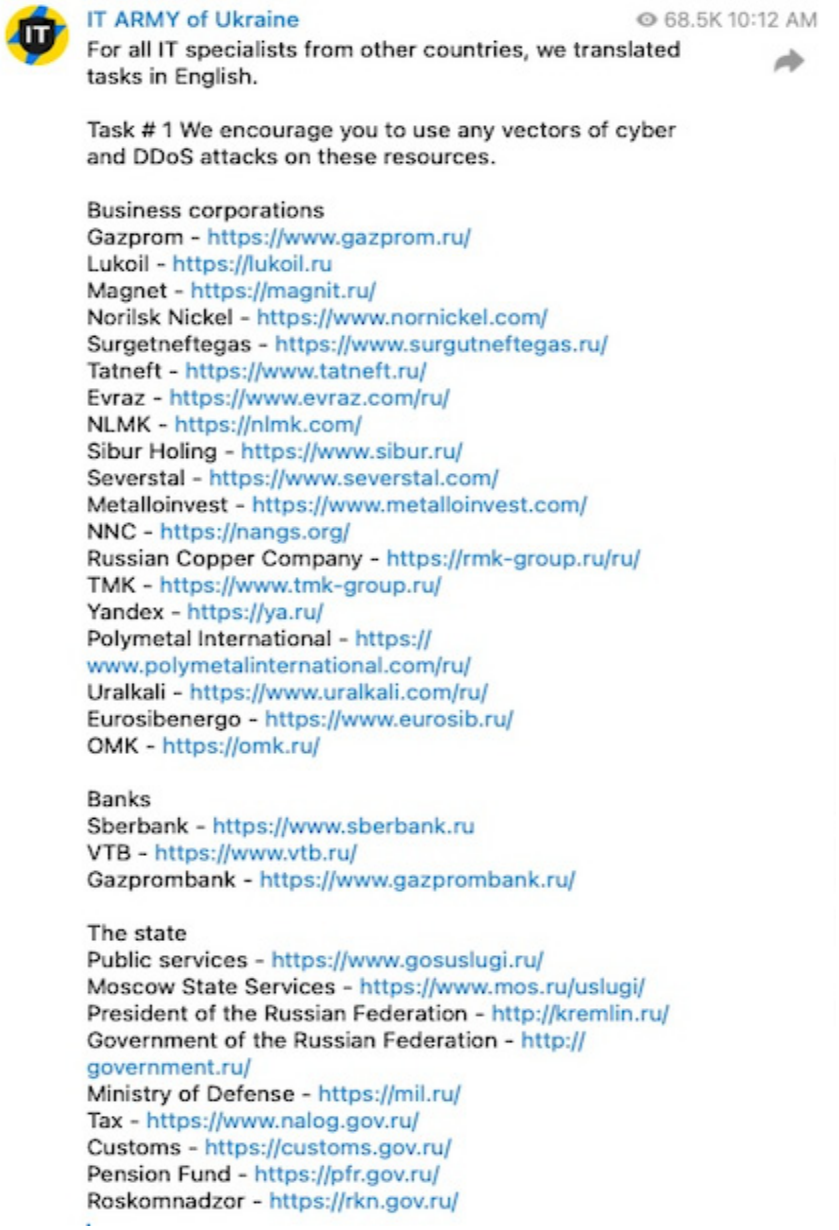
Unsurprisingly, the world's cybernews was dominated by the cyber aspects of Russia's invasion of Ukraine. We have been living through, and this TWiT podcast network has documented and chronicling, important and fascinating aspects of the evolution of the personal computer and the Internet. When this podcast began I was personally skeptical of the idea of cyber warfare. Since then I've been well disabused of any such skepticism. I've been interested to note that all of the experts I've heard speak about the possibility of cyber warefare feel much as I do, which is that it's something that no one is really that excited to unleash. As I said last week, the feeling is that no one has any real confidence in their own defenses being adequate. So no one wants to be the first to initiate what might be mutually assured cyber destruction.

Yet here we are today, picking around the edges of exactly that possibility. Since there isn't a huge amount to say about any single aspect of this, I'm not going to spend a lot of time on any one of them. But since the specter of cyber is very clearly hanging in the air, we shouldn't ignore it either.

On Saturday the 26th...

Ukraine's Minister for Digital Transformation, Mykhaylo Fedorov, announced the creation of an army of IT specialists to fight for Ukraine in cyberspace. Mykhaylo said: *"We have many talented Ukrainians in tech: developers, cyber-specialists, designers, copywriters, marketing specialists, targeting specialists, etc.* ["targeting specialists", yikes!] *We are creating an IT Army. All operational tasks will be posted here. There's plenty to do for everyone. We continue our fight at the cyber-front."*

And Mykhaylo's call did not go unheeded. Since creating the volunteer organization **over 175,000 people have subscribed.** Many have been tasked with launching DDoS attacks against Russian websites including government websites, banks, and energy companies. On February 27, officials also told volunteers to target websites registered in Belarus. Mykhaylo also publicly released the targeting list:



So, it's an open call for anyone and everyone to participate. But let's all be clear that the perceived justice of the cause doesn't make it legal.

According to Victor Zhora, an official at the Ukrainian cybersecurity agency charged with protecting government networks, *"Russian media outlets that are "constantly lying to their citizens," and financial and transportation organizations supporting the war effort, are among the potential targets for digital attacks from the so-called Ukrainian IT army."* He said that the "IT army" is a loose band of Ukrainian citizens and foreigners that are not part of the Ukrainian government — but Kyiv is encouraging them. It's an example of how the Ukrainian government is pulling out all the stops to try to slow Russia's military assault, and illustrates how cyberattacks have played a supporting role in the war. The goal of the "IT army" of Ukraine is to *"do everything possible … to make [the] aggressor feel uncomfortable with their actions in cyberspace and in Ukrainian land."*... this was Victor Zhora in a video conference with journalists Friday.

Ukrainian "Cyber Unit Technologies" is paying for attacks on Russia.
Given what I've been seeing in the news, it's unclear why you would need to give any Ukrainian hacker a bounty to encourage them to launch cyberattacks against Russia. Just making it legal is all I'd need. But last Tuesday, the Kyiv-based cybersecurity firm initiated a campaign to reward hackers for taking down Russian websites, pledging an initial $100,000 for the program.

Although, as we'll see next, many traditional criminal gangs have publicly expressed their allegiances, Cyber Unit Technologies emphasized that the company only seeks to work with locally known security experts — to prevent infiltration by Russian agents. If such hackers already had mature tools that they had been using for sanctioned red vs blue team exercises and drills they might well be able to retarget those tools. And you kinda have to imagine that Ukraine, being as much in Russia's cyber cross-hairs as they have been for the past 20 years, would have had occasion to develop and hone such tools. This is probably the reason why NATO's CCDCOE, their Cooperative Cyber Defense Centre of Excellence, wants Ukraine involved, but we'll get to that in a moment.

First, let's talk about **Hackers taking sides...**
As a result of Russia's determination to unilaterally and by sheer force attempt to illegally annex Ukraine as it previously annexed Crimea, we have the world's well-known hacking groups now squaring off and taking publicly declared sides for and against. Last Friday, Recorded Future's publication "The Record" described the declarations this way:

> *Russia's invasion of Ukraine has taken place both on and offline, blending physical devastation with escalating digital warfare. Ransomware gangs and other hacking groups have taken to social media to announce where their allegiances lie. The Record will be tracking who these groups align with, as well as any attacks they launch related to the conflict. Many of the pronouncements from these groups include threats against critical government infrastructure. Some collectives are state-sponsored while others are decentralized — but all are able to take down computer systems and breach organizations.*
>
> *Allan Liska, a ransomware expert at Recorded Future said: "It is now an inevitable part of any military action that so-called 'Cyber Patriots' will engage the perceived enemy either of their*

own free will or at the direction of their government. Some of these activities, such as Anonymous launching DDoS attacks, will be nothing more than minor nuisances but others could have real consequences. Ransomware groups, for example, have more targets than they can go after right now and may decide to focus on attacking the enemies of their country to create real disruption. And the more skilled groups can have an even greater impact." Liska warned that Sandworm and UNC1151 are the most concerning in terms of their capabilities and activity, and should be closely monitored.

Okay, so what do we know at the moment about whose on which side of this mess?

The well-known collective "**Anonymous**" declared via Twitter on February 24th that its collective is *"officially in a cyber war against the Russian government."* The group later tweeted that they had targeted the Russian-state controlled international television network RT, and *"has taken down the website of the Russian propaganda station RT News."*

"**Anonymous**" is a decentralized hacktivist group that targets different government institutions and government agencies, corporations, and the Church of Scientology. **GNG**, a hacking group affiliated with Anonymous, has gained access to SberBANK's database and leaked hundreds of its data files. Sberbank, Russia's largest lender, is now facing failure. **NB65** is another affiliate of Anonymous who Tweeted their support for Ukraine: *"#Anonymous is not alone. NB65 has officially declared cyber war on Russia as well. You want to invade Ukraine? Good. Face resistance from the entire world. #UkraineWar All of us are watching. All of us are fighting."*

And also as of February 28th, another group under the Anonymous umbrella named **DeepNetAnon** has joined in the operations against Russia by attacking and intercepting Russian radio receivers. The group tweeted: *"The Russians have now taken offline the second web server hosting a Software-Defined Radio receiver (used to interact with Radio Frequencies). Too bad there's many more sites we can use. (;"*. The collective also announced that they have successfully hacked the Ministry of Economic Development of Russia. **1LevelCrew** also showed their support for Ukraine and tweeted, *"TANGO DOWN – http://pfr.gov.ru – Pension Fund of Russian offline."* Another collective known as **HydraUG** made a clear statement via Twitter: *"I'm not here to deface/destroy your website, I'm here to liberate Ukraine."*

As of Wednesday, another affiliate named **N3UR0515** took to Twitter to declare support and call on YouTube to take down Russian propaganda. The group has administered DDoS attacks and taken down 'ria.ru' — the Official Russian Information Website. Joining the Anonymous collective, **VogelSec (v0g3ISec)** announced that they had hacked into the Russian Space Research Institute database and leaked files from RosCosmos, though the hack has not been confirmed.

Ghostsec announced their support for Ukraine: *"In support of the people in Ukraine WE STAND BY YOU!"* Also known as Ghost Security, the group considers itself a 'vigilante' group, and was initially formed to target ISIS websites that preach Islamic extremism. Ghostsec is also commonly referred to as an offshoot of Anonymous.

AgainstTheWest (ATW) – Is standing with Ukraine. The group's Twitter account says, *"We're back in action. Standing against Russia. Active until Russia stands down."* The group is actively working to breach Russian infrastructure including Russian railways and Russian Government

contractor "promen48[.]ru." On March 1st the group issued a new statement for further clarification, *"We won't be collaborating with anonymous. ATW will be splitting into two groups. One for Russia related breaches, one for Chinese related,"* the group states. ATW accused Anonymous of taking the credit for the work done by ATW: *"Anonymous has had a lot of media publicity over the years for hacking, and to see this. It didn't sit right."* ATW appears to have been suspended from Twitter as of last Thursday, March 3.

SHDWsec – which joins the movement to support Ukraine. The group is working in collaboration with **ATW** and **Anonymous** in operations against Russia, *"SHDWSec joined forces with @AgainstTheWest_ First stage is now on the roll. Expecting us is too late. Brace for impact. More to come."*

Belarusian Cyber Partisans – also supporting Ukraine. The activist hacking group successfully accessed the computers that control the Belarusian train system, stopping trains in Minsk and Orsha, as well as in the town of Osipovichi. The operation was intended to *"slow down the transfer"* of Belarus-based Russian troops into Ukraine. Over the past year, the hacktivists have worked against the Belarus government and were able to leak data of secret police archives, lists of alleged police informants, personal information about top government officials and spies, and more.

KelvinSecurity – also announced that they stand with Ukraine: *"I want to release this to support the digital war against RUSSIA. I have a list of weapons development documents that I took from a Russian ballistic institute and I also have internal videos from RT, and the Russian nuclear institute,"* the statement says. The group has been tweeting evidence of their engagement in cyber operations.

Raidforum2 – also stands with Ukraine. The group announced: *"Raidforums2 is in support of Ukraine. Members are actively DDOSing Russian websites and attacking Russian infrastructure. We also have reason to believe the Chinese are hacking Ukrainian networks."* Previously labeled as Raidforum, the collective is now operating as **Raidforum2** after having outage and access issues. It is unclear what went wrong with the original Raidforum.

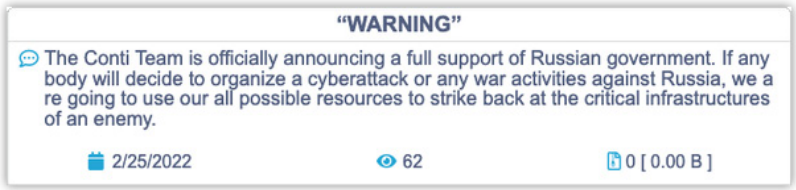
ContiLeaks — definitely not Conti, we'll get to them in a minute — back Ukraine. The group has exposed the infamous ransomware group **Conti** from the inside out. Following February 27th Conti statement of full Russian support, an account named **ContiLeaks** leaked hundreds of files containing internal Conti communications. The informant is believed to be Ukrainian and has continued to leak more and more files as days go by. More recent data shows communication depicting the chaos within Conti. Actor 1 says, *"Hi, all VM farms are cleared and deleted, servers are disabled."* Actor 2 responds, *"I deleted all the farms with the shredder and shut down the servers."*

Secjuice – stands with Ukraine. This cyber collective is taking a less volatile approach by using open-source intelligence (OSINT) and psychological operations (PsyOps). At the request of Ukraine's IT army, they're creating a website for missing persons within Ukraine as a resource for families. In a tweet on March 2, the group asked for assistance in ensuring the website is hosted on a safe server and not vulnerable to attack.

Okay, so there are a bunch of hacker collectives aligned with Ukraine against Russia. But Russia

has its defenders and offensive responders, too...

Of course, **Conti,** in full support of Russia. EmsiSoft's ransomware expert Brett Callow shared a tweet from the Conti gang:



"If anybody will decide to organize a cyberattack or any war activities against Russia, we are going to use our all possible resources to strike back at the critical infrastructures of an enemy."

As we know, the Conti ransomware gang is highly sophisticated and known for being the first group to weaponize the Log4Shell vulnerability and operate a fully-developed attack chain. But it appears that not everyone within Conti shared the group's loyalty to mother Russia. A few days after Conti announced their support for Russia, an insider, believed to be Ukrainian, leaked 400 files of internal communications between members of the group. The leaked messages go back more than one year to January 2021. The data was shared with the malware research group VX-Underground who have posted an archive of the leaked data on their site:

https://share.vx-underground.org/Conti/

The hacking collective, or the individual, leaking Conti information is now being referred to as **ContiLeaks**.

Minsk-based group '**UNC1151**' – supporting Russia. **UN1151** is believed to be state-sponsored by Belarus and has already been working to compromise the email accounts of Ukrainian military personnel. The group's members are officers of the Ministry of Defence of the Republic of Belarus. Facebook has taken down accounts used by **UNC1151** which targeted Ukrainian officials through Facebook posts that displayed videos depicting Ukrainian soldiers as weak. Facebook also blocked various phishing domains that were being used to jeopardize Ukrainian accounts.

Zatoichi – Is supporting Russia through the spread of disinformation via the group's Twitter account. Among many of their false claims, the account stated, *"Killnet has already taken down the Anonymous website, which announced the start of a cyber war with the Russian government, as well as the Right Sector website, and the website of the President of Ukraine."*

And speaking of **Killnet**, they also clearly stand with Russia. The group published a video addressing the people of Russia encouraging them to never doubt their country. The video features a hooded figure with a distorted voice claiming to have taken down the website belonging to Anonymous. Little is known about the group and it is unclear as to whether the group existed previously.

Then we have **XakNet** backing Russia and referring to themselves as a *"team of Russian patriots"* in a recent statement and criticized Anonymous, *"We do not hide behind the mask of*

abstract 'Anonymous'." The announcement concludes with a final threat, *"For every hack/DDoS in our country, similar incidents will occur in Ukraine."*

The **Stormous Ransomware** collective stands with Russia. Though their intent appears to have been somewhat lost in translation, they publicly announced, *"The STORMOUS team has officially announced its support for the Russian governments. And if any party in different parts of the world decides to organize a cyber-attack or cyber-attacks against Russia, we will be in the right direction and will make all our efforts to abandon the supplication of the West, especially the infrastructure. Perhaps the hacking operation that our team carried out for the government of Ukraine and a Ukrainian airline was just a simple operation but what is coming will be bigger!!"* The group has been around since the beginning of the year and is believed to be financially motivated. Their messages are in Arabic. More recently on March 1, the group issued a warning against "western unions" and more specifically companies in the U.S., after being attacked by unspecified U.S. companies causing their site to be shut down.

Digital Cobra Gang (DCG)'s public statement of support reads, *"DIGITAL COBRA GANG DCG has officially declared cyber war on hackers who attacking Russia as well and to protect justice. Do you want to invade Russia? Taste the good from the whole WORLD #Ukrainewar #Russia We fight for the Good, 10m deaths and 50 wars Russia? NO!"* This group first appeared via Twitter on February 27th and their most recent update declares their use of a 'secret weapon.' *"We set many traps so we have wired 27,918 computers from the guys who attacking Russia and we are ready to drop our secret weapon."*

Freecivilian is united with Russia. The group is reportedly advertising stolen data from 50 different Ukrainian government websites from a February 23 attack. The attacks on the websites included displayed defacement messages that were almost identical to messages from a January 15 attack linked to **UNC1151**. Although claiming to be an independent cybercriminal, many suspect the group is linked to nation-state actors.

SandWorm is backed by Russia. The group, known for its recent malware called Cyclops Blinks, is comprised of Russian state-sponsored hackers. They've been around for a while and have malware which targets WatchGuard Firebox firewalls.

The Red Bandits (cute name) Tweeted on February 22nd: *"We've hijacked the @UkrainePolice Dashcams and have been watching them. If Ukraine does not do what #Russia wants we will escalate our attacks against Ukraine to involve panic scares. We will also consider distributing ransomeware."* The collective self-identifies as a cybercrime group from Russia, however, it is widely speculated to in fact be Russian Intelligence.

Since their original strongly-worded statement, the group seems to be wavering in its threats against Ukraine. One week ago, March 1st, perhaps in response to what had transpired since their earlier tweet on the 22nd, the group tweeted: *"We want everyone from Ukraine to read this: We stand strongly with citizens of Ukraine and that's why we have not attacked anything other than their government. We also have not given a percentage of intel we have against Ukraine," the tweet continues in a long thread. "We do not respect Putin as a leader of Russia but we respect him as a citizen of Russia as we support every citizen. We do not agree with his unpeaceful actions against Ukraine as an operation."* The statement then continues in a later post, *"Please understand, we're not going to stop defending our country. We will not surrender*

because of reasons but we will not attack first, we'll defend attack meaning you guys hack Russia a few times we hack back. Simple, please understand we see Ukraine citizens as family."

Coomingproject – The international hacker group announced in a statement, *"Hello everyone this is a message we will help the Russian government if cyber attacks and conduct against Russia."* The gang is linked to the 2021 data breach and leak of the South African National Space Agency.

It was this raft of hacker group pronouncements that prompted Ukraine's Defense Ministry to solicit Ukraine's underground hacker community with a call-to-action encouraging Ukrainian hackers to assemble in a mission to protect the nation's critical infrastructure from cyberattacks and act offensively against Russia in cyber espionage operations.

StarLink in Ukraine

And back to Ukraine's Minister for Digital Transformation, the young Mykhaylo Fedorov: On February 26th, Mykhaylo tweeted to @elonmusk:

Although, so far, Ukraine's Internet access has been relatively stable, concerns over the possibility of widespread outages, as Russia has been increasingly attacking communications infrastructure, have recently increased. So, it was with some sense of relief that an equipment truck arrived from Starlink, the satellite Internet subsidiary of Elon Musk's SpaceX.

Will it be helpful? Or was it another P.R stunt for which Elon has become known? It's too soon to say. But more trucks, many more trucks, will be needed. According to Ukraine's Ministry of Digital Transformation, only one truck of Starlink kits has arrived in Ukraine. Now the Ministry is raising funds to purchase additional equipment, according to Forbes Ukraine. Ukraine is also considering the purchase of used Starlink devices. According to Business Insider, a standard Starlink kit costs $499 with a subscription to the network costing $99, presumably per month.

And so far, the system appears to be helping some Ukrainians stay connected. The general stability of the Ukrainian Internet service access allows Ukraine's President Volodymyr Zelensky

and other citizens to update the outside world about the Russian invasion of their sovereign territory.

But Internet connectivity has been affected in the southern and eastern regions of the country where fighting has been the heaviest. Ukrainian officials have stated that Russia would not be able to switch off internet access for the entire country, and Ukraine's multiple land fiber connections to the west makes it more difficult to take Ukraine off the Net as a whole.

Still, many Ukrainians fear they could be cut off from the world if Russian troops destroy the critical infrastructure responsible for television and the internet. It's amazing how much we take our continuous connectivity to the global network so much for granted now.

Control of the Internet and telephone communications can be of strategic value. Ukraine has limited Russian troops' access to networks by having its phone carriers — Kyivstar, Vodafone and Lifecell — shut down network access to phones from Russia and Belarus. So troops from those countries will be unable to send misleading messages or spread false information via phone calls.

Interestingly, Elon had apparently been having trouble obtaining a license to activate StarLink in Ukraine. One can imagine the political push back from the existing carriers who were in no hurry to increase their competition. But no one batted an eye when Elon said: "Give me permission to turn it on and I will." They did, and he did. Afterwards, a Ukrainian engineer Oleg Kutkov, said in an interview with the Verge that his Starlink dish got a signal from one of SpaceX's satellites in just 10 seconds. He told The Verge: "I honestly didn't believe that it would work."

Russia blocks access to Facebook, Twitter, foreign news outlets

And on the "two can play that game" line, Russia has blocked access to Facebook after Meta deactivated or restricted access to accounts belonging pro-Kremlin media outlets and news agencies, including RIA Novosti, Sputnik, and Russia Today. And our favorite Russian agency "Roskomnadzor" told Interfax that Russia has now also blocked access to Twitter (twitter.com) following a demand made by the Prosecutor General's Office.

On Thursday, Roskomnadzor asked Meta to immediately lift all restrictions on Russian media outlets members of the RT Media Group. Roskomnadzor said Friday that the decision was motivated by Facebook discriminating against Russian media and information resources starting with October 2020 — So, quite some time ago. Roskomnadzor stated "On March 4, a decision was made to block access to the Facebook network within the Russian Federation."

And also last Friday, Roskomnadzor also blocked access to multiple foreign news outlets, some of them designated as foreign agents, including Voice of America, BBC, DW, and Radio Free Europe/Radio Liberty. Not that they had to, but Russia justified the media outlets' ban saying that they spread fake news regarding the ongoing invasion of Ukraine, the methods used by its military against Ukrainian civilians and infrastructure, and the number of casualties suffered by the Russian army. I've seen a great deal of the coverage. I'm unsurprised that they would not want all Russians to see what we're seeing here in the West.

Google was also asked on Thursday to stop advertising campaigns spreading what Roskomnadzor called "misinformation" on YouTube videos about the Russian invasion of Ukraine. Roskomnadzor said that online ads with no age labels and inaccurate content are being used to

instill "protest moods" and spread false info on the Russian "special operation" in Ukraine.

YouTube has become quite important, so Roskomnadzor sent a letter to Google LLC demanding that Google immediately stop disseminating false information of a political nature about the special operation of the Russian Armed Forces in Ukraine on the territory of Russia. <unquote> That's rich. Roskomnadzor's demand continued, saying: “Such advertising messages are shown to the Russian users of the video hosting site YouTube and contain misinformation aimed at forming a distorted perception of the events taking place and creating protest sentiments among the Russian Internet audience. The agency considers it unacceptable to use YouTube in the information war against Russia, including using the advertising capabilities of the platform.”

Roskomnadzor also notified all independent Russian media outlets not to spread false information about the shelling of Ukrainian cities, as well calling the "ongoing operation" an attack, invasion, or a declaration of war. And I'm sure everyone has probably heard by now, Russia is planning to introduce a new law that would punish spreading fake news about the Russian armed forces' military operations in Ukraine with up to 15 years in prison.

For their part, Google has already taken action to stop actual misinformation, taking down disinformation campaigns regarding Russia's invasion, and blocked YouTube channels belonging to Russia Today (RT) and Sputnik across Europe at the request of European Union authorities. Roskomnadzor protested YouTube's decision, demanding the immediate removal of all access restrictions to the official accounts of Russian media (including RT and Sputnik) in Europe.

Previously, Google demonetized Russian state-funded media across all its platforms to block Russian state-funded media from running ad campaigns. And YouTube has removed hundreds of channels with thousands of videos which violate its Community Guidelines, including channels engaging in coordinated deceptive practices. Google said: “When people around the world search for topics related to the war in Ukraine on Search or YouTube, our systems prominently surface information, videos and other key context from authoritative news sources.” For the time being, Google said that most of its services, including Search, YouTube, and Maps, remain available in Russia to provide Russians with access to global information and perspective.

Overall, the situation appears to be developing as we would have expected it would: The providers of the content hold all of the cards. They, and they alone, are able to decide which content their platforms serve up and which they block and delete. The only power a local authoritarian government has is to block everything

Google has become proactive

And speaking of Google... They announced last Tuesday that they were focusing upon increasing security measures to help protect Ukrainian civilians and websites which other US technology providers, like Meta, had also been doing. Meta has been actively working to disrupt the flow of disinformation in the region and take down accounts that targeted Ukrainian officials with phishing attempts.

But as for Google, in a statement by Kent Walker, their President of Global Affairs, Google said the measures include SOS alerts on its Search function, automated detection and blocking of suspicious activity, Gmail notifications of government-backed attack warnings, increased

authentication challenges, and the expansion of its Advanced Protection and Project Shield programs. In other words, a rapid and strengthening of authentication.

As for Google's Search and Maps functions, the company has disabled various live Google Maps features within Ukraine — such as traffic information — to prevent public access to population densities within different areas. The company also issued SOS alerts that will guide users to United Nations resources for refugees and asylum seekers when they search for refugee and evacuation instructions. So they've been more carefully curating their search engine results. And they have reportedly "expanded security protections" after its Threat Analysis Group reported an increased focus from threat actors on Ukrainian targets. They've blocked attempted attacks without "any compromise of Google accounts as a result of this campaign."

Google also increased the frequency of authentication challenges for Ukrainian civilians and is relying on its Advanced Protection Program to safeguard hundreds of high-risk accounts in the area. A campaign known as Project Shield is also being used to help protect over 100 websites belonging to news publications, human rights groups, political organizations, and other groups that are targeted by distributed denial-of-service attacks.

And following the statement issued by Google last Tuesday, Apple announced that they had ceased all sales of their technology in Russian online stores after Ukraine's Vice Prime Minister pleaded with them to shut down the app store and halt all Russian sales.

Namecheap says "no more"

Eight days ago, the Phoenix, Arizona based domain registrar "Namecheap", which was founded 22 years ago in 2000 and is now operating in 18 countries with 1700 employees and managing 14 million domains, sent the following eMail to all of their registrants located in Russia:

> *"Unfortunately, due to the Russian regime's war crimes and human rights violations in Ukraine, we will no longer be providing services to users registered in Russia. While we sympathize that this war may not affect your own views or opinion on the matter, the fact is, your authoritarian government is committing human rights abuses and engaging in war crimes so this is a policy decision we have made and will stand by. If you hold any top-level domains with us, we ask that you transfer them to another provider by March 6, 2022.* [So, a 7-day notice of unilateral service cancellation. They continue...]
>
> *Additionally, and with immediate effect, you will no longer be able to use Namecheap Hosting, EasyWP, and Private Email with a domain provided by another registrar in Russian TLDs. All websites will resolve to 403 Forbidden, however, you can contact us to assist you with your transfer to another provider."*

Predictably, yhis eMail generated some angry pushback from Russians, to which Namecheap's CEO replied over on Ycombinator: https://news.ycombinator.com/item?id=30505495

> *"We haven't blocked the domains, we are asking people to move. There are plenty of other choices out there when it comes to infrastructure services so this isn't "deplatforming". I sympathize with people who are not pro-regime, but ultimately even those tax dollars they*

may generate go to the regime. We have people on the ground in Ukraine being bombarded now, non-stop. I cannot with good conscience continue to support the Russian regime in any way, shape or form. People that are getting angry need to point that at the cause, their own government. If more grace time is necessary for some to move, we will provide it. Free speech is one thing, but this decision is more about a government that is committing war crimes against innocent people that we want nothing to do with."

I'll just note that expecting anyone in Russia to successfully move their domain at this moment with banks closed, Visa, MasterCard and Paypal all having suspended services, and the value of the Russian ruble having collapsed, is not practical. So, in practice, it really does represent effective abandonment.

For what it's worth, I feel a bit queasy about that. It seems to me that individual Russian citizens, small businesses, charitable organizations, etc. ought to have the West standing with them to help them survive this period, rather than abandoning them in their time of greatest need. All indications are that Russian citizenry is quite divided in their feelings about the actions of their own regime. Being politically aware in the U.S., we certainly understand the nature of division. There are many topics of discussion which are now strictly off limits between my own beloved family members. We, too, are a divided nation. But when Namecheap took their Russian customer's money they didn't ask about their political sentiments. They took their money in return for a promise to provide service for some period of time. Commitments are not subject to reconsideration. That's what makes them a commitment. I would have no problem if Namecheap were to announce that they would be suspending the renewal of domains at their expiration, so giving their Russian customers fair notice of the need to find another service at that time. I didn't see Namecheap offering to refund their customers' money in US Dollars, which are now quite valuable at the current dollars-to-rubles exchange rate. But even doing that would still have left those customers stranded.

Namecheap also says yes

And two days later, at 4:27am on March 2nd, Namecheap tweeted: *"Effective immediately, we will begin offering free anonymous hosting and domain name registration to any anti-Putin anti-regime and protest websites for anyone located within Russia and Belarus. Please contact our support for details."*

Since this announcement followed two days after their Russia abandonment eMail, reading between the lines, I'd bet that this is their way of selectively backpedaling and arranging to continue offering domain services and hosting to only those entities whose politics they're aligned with.

Telegram's use explodes

We've been talking about Telegram for the past 9 years, ever since it first appeared in 2013. Despite its popularity, I've always looked askance at it, since its authors unnecessarily violated the cardinal rule of cryptography: They rolled their own — unlike the many other properly designed alternatives such as Signal and Threema. And offering a bounty for someone who cracks their crypto is not the same as designing it properly. For all we know, it has been cracked by someone like the NSA, and the knowledge they have, and the access this provides, is worth far more to them than Telegram's bounty. They would want it to remain just the way it is,

presumably unexamined, apparently unbroken and certainly not fixed.

But about this, no one could care less what I think. Telegram is super popular and its popularity has recently exploded during this horrific Russia/Ukraine mess.

As we've followed Roskomnadzor's and the Russian Federal Security Service's (the FSB's) ultimately futile efforts through the years to shutdown and block Telegram, they finally gave up two years ago. The risk intelligence company, Flashpoint, noted in a recent report that 6 out of 10 Russians use Telegram precisely because their country's authorities can't impose their oversight on the platform. No surprise there.

So it should also be no surprise that Telegram's messaging has taken a pivotal role in the ongoing conflict between Russia and Ukraine and is being widely used by both hacktivists and cybercriminals. According to a report from CheckPoint, the number of Telegram groups has increased **sixfold** since February 24 and some of them, dedicated to certain topics, have exploded in size, in some cases counting more than 250,000 members.

Three categories which have rapidly gained in popularity as a direct result of the Russian invasion of Ukraine are:

- Volunteer hackers engaged in DDoS and other kinds of cyberattacks against Russian entities.
- Fundraising groups that accept cryptocurrency donations, allegedly for Ukrainian support.
- And various "news feeds" that promise to offer reliable reports from the front-line.

We've already talked about the group that stands out among those that lead the anti-Russia cyber-warfare operations: The so-called "IT Army of Ukraine", whose membership is now at 269,972. In addition to targeting, orchestrating and launching DDoS attacks against key Russian sites, the group exposes the personal details of opinion-makers in Russia and other people who play a significant role in the conflict.

As for the "fund-raising groups" — that's in air quotes because, naturally and unfortunately, the majority of the self-declared "donation support" groups in Telegram are scams that take advantage of sentiments to relieve people of their money.

And then there's the "news" (also in air quotes). CheckPoint's coverage of Telegram notes:

> *In the era of social media, traditional news channels are merely a side show for numerous news feed telegram groups. These groups on Telegram report unedited, non-censored feeds from war zones, 24 hours a day, including footage that traditional mainstream media often refrained from airing live. In fact, about 71% of the groups we see are dedicated to news around the current conflict.*
>
> *CheckPoint researchers observed such groups appearing rapidly from the beginning of the conflict and have continued to grow since then. In such groups, the quality of news feeds is not a factor and users often leverage this to spread "news" and "facts" that are not verified, or checked. This is a form of psychological weapon, used to demoralize and influence moral.*

The bottom line is to be skeptical, use your own judgment, and guard against becoming seduced by anyone's narrative that seems too good to be true. It may indeed be too good to be true.

Michael Horowitz, a geopolitical and security analyst who's the head of Intelligence for the firm LeBeck International recently tweeted:

> *"I have deleted footage of a plane being shot down above Kharkiv as it seems to be from a video game. That's a very realistic one. Sorry for the mistake."*

Microsoft also shuts down in Russia

Last Friday, Microsoft's Chairman and President Brad Smith posted: *"Microsoft suspends new sales in Russia"* and in his posting he also weighs in on recent cyber attacks and defenses.The more interesting bits of news are at the beginning. Brad writes:

> *Like the rest of the world, we are horrified, angered and saddened by the images and news coming from the war in Ukraine and condemn this unjustified, unprovoked and unlawful invasion by Russia. I want to use this blog to provide an update on Microsoft's actions, building on the blog we shared earlier this week. We are announcing today that we will suspend all new sales of Microsoft products and services in Russia.*
>
> *In addition, we are coordinating closely and working in lockstep with the governments of the United States, the European Union and the United Kingdom, and we are stopping many aspects of our business in Russia in compliance with governmental sanctions decisions.*
>
> *We believe we are most effective in aiding Ukraine when we take concrete steps in coordination with the decisions being made by these governments and we will take additional steps as this situation continues to evolve. Our single most impactful area of work almost certainly is the protection of Ukraine's cybersecurity. We continue to work proactively to help cybersecurity officials in Ukraine defend against Russian attacks, including most recently a cyberattack against a major Ukrainian broadcaster.*
>
> *Since the war began, we have acted against Russian positioning, destructive or disruptive measures against more than 20 Ukrainian government, IT and financial sector organizations. We have also acted against cyberattacks targeting several additional civilian sites. We have publicly raised our concerns that these attacks against civilians violate the Geneva Convention.*

Coinbase

Last Sunday the 6th, Paul Grewal, the Chief Legal Officer for Coinbase announced the employment of crypto tech to promote sanctions compliance.

They announced that they're blocking access to more than 25,000 blockchain addresses — in other words, wallets — linked to Russian individuals and entities. And Coinbase shared all of the blocked addresses with the US government in order to further support sanctions enforcement. They will also be blocking sanctioned entities from opening new accounts and actively detecting attempts to evade the ban. The ban addresses sanction lists maintained by countries worldwide, including the United States, United Kingdom, European Union, United Nations, Singapore, Canada, and Japan.

Citing an example, Paul Grewal wrote: "For example, when the United States sanctioned a Russian national in 2020, it specifically listed three associated blockchain addresses. Through

advanced blockchain analysis, we proactively identified over 1,200 additional addresses potentially associated with the sanctioned individual, which we added to our internal blocklist. Today, Coinbase blocks over 25,000 addresses related to Russian individuals or entities we believe to be engaging in illicit activity, many of which we have identified through our own proactive investigations."

Two weeks ago, on February 27th, Ukraine's Mykhailo Fedorov asked for more than the crypto exchanges were willing to do. He tweeted: *"I'm asking all major crypto exchanges to block addresses of Russian users. It's crucial to freeze not only the addresses linked to Russian and Belarusian politicians, but also to sabotage ordinary users."*

But Coinbase and the other crypto exchanges, including Binance, refused to freeze all Russian users' accounts. Their various spokespeople added that while they will not block all Russian accounts on their platforms, the crypto exchanges will take steps to identify all sanctioned entities and individuals and block their accounts and transactions.

Coinbase cited the "economic freedom in the world" and Binance said it was about the "greater financial freedom for people across the globe" and banning users' access to their cryptocurrency "would fly in the face of the reason why crypto exists."

Russia releases the IP addresses and Domains of DDoS attacks
Last Thursday, amid the continually escalating Russian attack on Ukraine, Russia's NCCCI, their "National Coordination Center for Computer Incidents," published a list, presumably intended to be used by those sympathetic to President Putin's expansionist agenda for retaliation against these claimed attacks on Russian cyber infrastructure.

I say, "claimed attacks" because, in addition to the massive list containing 17,576 IP addresses were 166 domains that the NCCCI said are behind a series of DDoS attacks aimed at its domestic infrastructure. And among those domains were the U.S. Federal Bureau of Investigation (FBI), the Central Intelligence Agency (CIA), and websites of several media publications including USA Today and Ukraine's Korrespondent magazine. So it appears that not liking someone is enough to get them on the list.

Not surprisingly, the NCCCI is reacting to the gradual and incremental but also probably inevitable withdrawal of Western and non-Russian cyber services from Russia. As part of its recommendations to counter the DDoS attacks, the agency is urging organizations to "ringfence" network devices (whatever that is), enable logging and change passwords, enforce data backups, and be extra alert for phishing attacks.

The coolest advice caught me a bit by surprise, but I thought it was really interesting and obvious in retrospect. The NCCCI advised its citizenry and Russian enterprises to turn off automatic software updates and disable third-party plugins on websites.

At this point, Microsoft has pulled the plug on Russian revenue, but the US is not at war with Russia. However — wow — consider the implications of Microsoft's deliberate sabotage of Windows in aid of a war effort against Russia. I would not want to be on their side.
And this puts a spin I had never considered on my rooting for having all of our devices phoning home and auto-updating all the time. We don't want to go to war with China, either. We could

easily be on the receiving end with all of the IoT gadgets most of us are now using. This is all quite sobering. It's one thing to have an inadvertent security mistake. It's another thing to have a deliberate attack. I was slow to buy into this whole cyberwar idea. So I suspect that I'm probably still being too naïve.

The NCCCI also advised its citizenry to *"Use Russian DNS servers. Use the corporate DNS servers and/or the DNS servers of your telecom operator in order to prevent the organization's users from being redirected to malicious resources or other malicious activity. If your organization's DNS zone is serviced by a foreign telecom operator, transfer it to the information space of the Russian Federation."*

And there, again, Russian devices are necessarily trusting the certificates issued by Western certificate authorities since the websites and services that Russians depend upon are serving Western certificates.

Just think for a minute how much implicit cross-border trust there is in today's globally interconnected world. This has been the background thought I've had all throughout this mounting aggression: It's really no longer in any way practical for any single country to completely isolate itself from the rest of the world. There's just too much true interdependence.

And speaking of interdependence, according to the global Internet access watchdog NetBlocks, Russia has placed extensive restrictions on Facebook access within the country. And late last week, there were reports that Twitter was also unavailable.

Ukraine also updated its list of targets for its volunteer "IT Army" of civilian hackers. Now on the list are the Belarusian railway network, Russia's homegrown satellite-based global navigation system GLONASS, and telecom operators like MTS and Beeline.

Russia to permit software piracy

Meanwhile, Russian authorities are drafting a set of measures to support the country's economy against the pressure of foreign sanctions, and as part of this, the proposal would eliminate intellectual property right limitations, thus permitting piracy.

The plan is to establish a "unilateral" software licensing mechanism that would renew expired licenses without requiring the consent of the copyright or patent owner. This new process will be available in cases where the copyright holder is from a country that has supported sanctions against Russia for products without Russian alternatives — which are many. This move is Russia's response to numerous software vendors exiting the Russian market and suspending new license sales including Microsoft, Cisco, Oracle, NVIDIA, IBM, Intel, and AMD.

The original Article 1360 of the Civil Code of the Russian Federation says that: *"In the interests of national security the Government of the Russian Federation shall have the right to permit the use of an invention, utility model, or industrial design without the consent of the patent holder provided that he is notified as soon as possible and payment to him a reasonable remuneration."* How, however, in multiple proposed amendments to the Russian Civil Code, the Russian Ministry of Digital Transformation wants to bypass compensation to license holders who are under sanction restrictions so that they can continue using the software.

Translated proposed amendments read: *"Amending Article 1360 of the Civil Code of the Russian Federation regarding the use of a license and other types of rights and the abolition of compensation to foreign companies originating from states that have acceded to the sanctions Federal Law."*

Of course, software products that rely on cloud services or online verification, as so many do now, will stop working since no unilateral change in Russia's international intellectual property treaties will keep online services from being shut down. But this does feel as though Russia will be entering a dark age. Who would want to sell to such a rogue nation even if sanctions were not in place?

Will Russia Disconnect?
Are we about to see Russia flip the switch?

Although Roskomnadzor has been working overtime to censor information by blocking its citizens' access to Western media, services such as Telegram have withstood all previous blocking attempts, and YouTube remains the #1 most popular service in all of Russia. Google is refusing to comply with Roskomnadzor's censorship demands while simultaneously blocking Russia's own state-sponsored propaganda. So it may be that nothing short of disconnecting all of Russia from the rest of the Internet will be the only workable solution.

I've previously talked about the RU.net, Russia's sovereign Internet, which has been in development for years and was successfully tested for actual deployment with the collaboration of all large internet providers in the country last summer. Remember when we discussed the need for and their establishment of any entirely autonomous DNS system.

Well, this past Sunday afternoon, a letter allegedly leaked from the Deputy Minister of Digital Marketing and Mass Communications of the Russian Federation was posted by Anonymous on Twitter. Since it's written in Russian, of course, I cannot read what it says. But Anonymous claims that it provides instructions to all organizations about how to prepare for connection to the runet and disconnection from the Internet:

"Russia is preparing to disconnect from the global internet, limiting access to information for the Russian people. That means censorship, and we are totally against censorship of any kind. So... let's turn up the pressure!" https://twitter.com/LatestAnonPress/status/1500589900193832966
— Anonymous (@LatestAnonPress) March 6, 2022

It would seem to me that "turning up the pressure" would only hasten the pulling of the plug. Russia doesn't have, and must import, Western technology. They cannot duplicate our semiconductors. But, unfortunately, they may have reason to count on China as a strategic partner. China really is the wildcard in much of this. But China is not the West and cannot replace much of what only Europe, the US and others provide. **We live in interesting times.**