The World Economic Forum's Partnerships Can Threaten Privacy

Analysis by Whitney Webb

With many focusing on tomorrow's Cyber Polygon exercise, less attention has been paid to the World Economic Forum's real ambitions in cybersecurity — to create a global organization aimed at gutting even the possibility of anonymity online. With the governments of the US, UK and Israel on board, along with some of the world's most powerful corporations, it is important to pay attention to their endgame, not just the simulations.

Amid a series of warnings and simulations in the past year regarding a massive cyber attack that could soon bring down the global financial system, the "information sharing group" of the largest banks and private financial organizations in the United States warned earlier this year that banks "will encounter growing danger" from "converging" nation-state and criminal hackers over the course of 2021 and in the years that follow.

The organization, called the Financial Services Information Sharing and Analysis Center (FS-ISAC), made the claim in its 2021 "Navigating Cyber" report, which assesses the events of 2020 and provides a forecast for the current year. That forecast, which casts a devastating cyber attack on the financial system through third parties as practically inevitable, also makes the case for a "global fincyber [financial-cyber] utility" as the main solution to the catastrophic scenarios it predicts.

Perhaps unsurprisingly, an organization close to top FS-ISAC members has recently been involved in laying the groundwork for that very "global fincyber utility" — the World Economic Forum, which recently produced the model for such a utility through its Partnership against Cybercrime (WEF-PAC) project.

Not only are top individuals at FS-ISAC involved in WEF cybersecurity projects like Cyber Polygon, but FS-ISAC's CEO was also an adviser to the WEF-Carnegie Endowment for International Peace report that warned that the global financial system was increasingly vulnerable to cyber attacks and was the subject of the first article in this 2-part series.

Another article, published earlier this year at Unlimited Hangout, also explored the WEF's Cyber Polygon 2020 simulation of a cyber attack targeting the global financial system. Another iteration of Cyber Polygon is due to take place tomorrow July 9th and will focus on simulating a supply chain cyber attack.

A major theme in these efforts has not only been an emphasis on global cooperation, but also a merging of private banks and/or corporations with the State, specifically intelligence and law enforcement agencies.

In addition, many of the banks, institutions and individuals involved in the creation of these reports and simulations are either actively involved in WEF-related efforts to usher in a new global economic model of "stakeholder capitalism" or are seeking to imminently introduce, or are actively developing, central bank-backed digital currencies, or CBDCs.

In addition, and as mentioned in the first article in this series, a cyber attack like those described in these reports and simulations would also provide the perfect scenario for dismantling the current failing financial system, as it would absolve central banks and corrupt financial institutions of any responsibility.

The convergence of several concerning factors in the financial world, including the end of LIBOR at the end of year and the imminent hyperinflation of globally important currencies, suggests that the time is ripe for an event that would not only allow the global economy to "reset", but also absolve the fundamentally corrupt financial institutions around the world from any wrongdoing.

Instead, faceless hackers can be blamed and, given recent precedents in the US and elsewhere, any group or nation state can be blamed with minimal evidence as politically convenient. This report will closely examine both FS-ISAC's recent predictions and the WEF Partnership against Cybercrime, specifically the WEF-PAC's efforts to position itself

as the cybersecurity alliance of choice if and when such a catastrophic cyber attack cripples the current financial system.

Of particular interest is the call by both FS-ISAC and the WEF Partnership against Cybercrime to specifically target cryptocurrencies, particularly those that favor transactional anonymity, as well as the infrastructure on which those cryptocurrencies run. Though framed as a way to combat "cybercrime", it is obvious that cryptocurrencies are to be unwanted competitors for the soon-to-be-launched central bank digital currencies.

In addition, as this report will show, there is a related push by WEF partners to "tackle cybercrime" that seeks to end privacy and the potential for anonymity on the internet in general, by linking government-issued IDs to internet access. Such a policy would allow governments to surveil every piece of online content accessed as well as every post or comment authored by each citizen, supposedly to ensure that no citizen can engage in "criminal" activity online.

Notably, the WEF Partnership against Cybercrime employs a very broad definition of what constitutes a "cybercriminal" as they apply this label readily to those who post or host content deemed to be "disinformation" that represents a threat to "democratic" governments.

The WEF's interest in criminalizing and censoring online content has been made evident by its recent creation of a new **Global Coalition for Digital Safety** to facilitate the increased regulation of online speech by both the public and private sectors.

FS-ISAC, Its Influence and Its Doomsday "Predictions" for 2021

FS-ISAC **officially exists** to "help ensure the resilience and continuity of the global financial services infrastructure and individual firms against acts that could significantly impact the sector's ability to provide services critical to the orderly function of the global economy."

In other words, FS-ISAC allows the private financial services industry to decide on and coordinate sector-wide responses regarding how financial services are provided during and after a given crisis, including a cyber attack. It was tellingly created in 1999, the same year that the Glass-Steagall Act, which regulated banks after the onset of the Great Depression, was repealed.

Though FS-ISAC's members are not publicly listed on the group's website, they do acknowledge that their membership includes some of the world's largest banks, Fintech companies, insurance firms and payment processors.

On their board of directors, the companies and organizations represented include CitiGroup, Bank of America, Wells Fargo and Morgan Stanley, among others, strongly suggesting that FS-ISAC is largely a Wall Street-dominated entity. SWIFT, the society that manages inter-bank communication and dominates it globally, is also represented on FS-ISAC's board.

Collectively, FS-ISAC members represent $35 trillion in assets under management in more than 70 countries. FS-ISAC also has ties to the World Economic Forum due to the direct involvement of its then-CEO Steve Silberstein in the WEF-Carnegie initiative and FS-ISAC's participation in the initiative's "stakeholder engagements."

There is also the fact that some prominent FS-ISAC members, like Bank of America and SWIFT, are also members of the WEF's Centre for Cybersecurity, which houses the WEF Partnership against Cybercrime project. At the individual level, the founding director of FS-ISAC, Charles Blauner, is now an agenda contributor to the WEF who previously held top posts at JP Morgan, Deutsche Bank and CitiGroup.

He currently is a partner and CISO-in-residence of Team8, a controversial start-up incubator that operates as a front for Israeli military intelligence in tech-related ventures that is part of the WEF Partnership against Cybersecurity. Team8's CEO and co-founder and the former commander of Israeli intelligence outfit Unit 8200, Nadav Zafrir, has contributed to WEF Centre for Cybersecurity policy documents and WEF panels on the "Great Reset".

In addition, current FS-ISAC board member Laura Deaner, CISO of Northwestern Mutual, served as the co-chair for the WEF's Global Futures Council on Cybersecurity. Teresa Walsh, the current global head of intelligence for FS-ISAC, will be a speaker at the WEF's Cyber Polygon 2021 regarding how to develop an international response to ransomware attacks. Walsh previously worked as an intelligence analyst for Citibank, JP Morgan Chase and the US Navy.

The FS-ISAC's recent report is worth looking at in detail for several reasons, with the main one being the sheer power and influence that its members, both known and unknown, hold over the current fiat-based financial system. The full report is exclusive to FS-ISAC members, but a "thematic summary" is publicly available.

The FS-ISAC's recent report on "Navigating Cyber" in 2021 is "based on the contributions of our members and the resulting trend analysis by FS-ISAC's Global Intelligence Office (GIO)" and includes several "predictions" for the current calendar year.

The group's GIO, led by Teresa Walsh, soon-to-be speaker at Cyber Polygon 2021, also "coordinates with other cybersecurity organizations, companies and agencies around the world" in addition to its intelligence gathering from FS-ISAC members.

At the beginning of 2020, when the COVID-19 crisis resulted in an overt push towards digitization, FS-ISAC launched a "new secure chat and intelligence sharing platform" that "provided a new way for members to discuss threats and security trends." It is fair to assume that the private discussions on this platform directly informed this report.

According to the recent FS-ISAC report, the main trends and threats discussed by its members through this service over the past year were "third party risks", such as the risk presented by major hacks of third party service providers, like the SolarWinds hack, and "geopolitical tensions."

The report contains several "predictions for 2021 and beyond." The first of these predictions is that adversarial nation-states will team up with "the cybercriminal underworld" in order to "obfuscate their activity and complication attribution."

FS-ISAC does not provide evidence of this having happened, but supporting this claim makes it easier to blame state governments for the activities of cybercriminals when politically convenient without concrete evidence. This has happened on several occasions with recent high-profile hacks, most recently with SolarWinds.

As noted in previous reporting, prominent companies that contract for the US government and military, like Microsoft, and intelligence-linked cybersecurity companies, are often the sole sources for such narratives in the past and, in those cases, do not provide evidence, instead qualifying such assertions as "likely" or "probable."

Even mainstream outlets reporting on FS-ISAC's "predictions" noted that "FS-ISAC did not point to specific examples of spies relying on such tradecraft in the past," openly suggesting that there is little factual basis to support this claim.

Other predictions focus on how third party service providers, such as SolarWinds and the more recently targeted Kaseya, will dominate, affecting potentially many thousands of companies across multiple sectors at once.

However, the SolarWinds hack was not properly investigated, merely labeled by US intelligence as having "likely" ties to "Russian" state-linked actors despite no publicly available evidence to support that claim. Instead, the SolarWinds hack appears to have been related to its acquisition of an Israeli company funded by intelligence-linked firms, as discussed in this report from earlier this year.

SolarWinds acquired the company, called Samanage, and integrated its software fully into its platform around the same time that the backdoor used to execute the hack was placed into the SolarWinds platform that was later compromised.

FS-ISAC also predicts that attacks will cross borders, continents, and verticals, with increasing speed. More specifically, it states that the cyber pandemic will begin with cyber criminals that "test attacks in one country and quickly scale up to multiple targets in other parts of the world." FS-ISAC argues that it is therefore "critical to have a global view on cyber threats facing the sector in order to prepare and defend against them."

Since FS-ISAC made this prediction, cyber attacks and especially ransomware have been occurring throughout the world and targeting different sectors at a much more rapid pace than has ever been seen before. For instance, following the Colonial Pipeline hack in early May, Japan, New Zealand, and Ireland all experienced major cyber attacks, followed by the JBS hack on June 1.

The hack of Kaseya, believed by some to be just as consequential and damaging as SolarWinds, took place about a month later on July 2, affecting thousands of companies around the world. The final, and perhaps the most important, of these predictions is that "economic drivers towards cybercrime will increase."

FS-ISAC claims that the current economic situation created by COVID-related lockdowns will "make cybercrime an ever more attractive alternative," noting immediately afterwards that "dramatic increases in cryptocurrency valuation may drive threat actors to conduct campaigns capitalising on this market, including extortion campaigns against financial institutions and their customers."

In other words, FS-ISAC views the increase in the value of cryptocurrency as a direct driver of cybercrime, implying that the value of cryptocurrency must be dealt with to reduce such criminal activities. However, the data does not fit these assertions as the use of cryptocurrency by cybercriminals is low and getting lower.

For instance, one recent study found that only 0.34% of cryptocurrency transactions in 2020 were tied to criminal activity, down from 2% the year prior. Though the decrease may be due to a jump in cryptocurrency adoption, the overall percentage of crime-linked crypto transactions is incredibly low, a fact obviously known to FS-ISAC and its members.

However, cryptocurrency does present a threat to the plans by FS-ISAC members and its partners to begin producing digital currencies controlled either by approved private entities (like Russia's Sbercoin) or central banks themselves (like China's digital yuan).

The success of that project depends on neutering the competition, which is likely why FS-ISAC subtitled its 2021 report as "the case for a global fincyber utility," with such a

utility framed as necessary to defend the financial services industry against cyber threats.

The WEF's Partnership Against Cybercrime

Conveniently for FS-ISAC, there is already a project that hopes to soon become this very global fincyber utility – the WEF Partnership Against Cybercrime (WEF-PAC). Partners in WEF-PAC include some of the world's largest banks and financial institutions, such as Bank of America, Banco Santander, Sberbank, UBS, Credit Suisse and the World Bank, as well as major payment processors such as Mastercard and PayPal.

Also very significant is the presence of all of the "Big Four" global accounting firms: Deloitte, Ernst & Young, KPMG and PricewaterhouseCoopers.

Think tanks/non-profits, including the Council of Europe, Third Way and the Carnegie Endowment for International Peace as well as the WEF itself, are also among its members as are several national government agencies, like the US Department of Justice, FBI and Secret Service, the UK's National Crime Agency and Israel's National Cyber Directorate.

International and regional law enforcement agencies, such as INTERPOL and EUROPOL, both of which are repeat participants in the WEF's Cyber Polygon, are also involved.

Silicon Valley is also well represented with the presence of Amazon, Microsoft, and Cisco, all three of which are also major US military and intelligence contractors. Cybersecurity companies founded by alumni and former commanders of Israeli intelligence services, such as Palo Alto Networks, Team8 and Check Point, are also prominent members.

The Israeli intelligence angle is especially important when examining WEF-PAC, as one of its architects and the WEF's current Head of Strategy for Cybersecurity is Tal Goldstein, though his biography on the WEF website seems to claim that he is Head of Strategy for the WEF as a whole.

Goldstein is a veteran of Israeli military intelligence, having been recruited through Israel's Talpiot program, which feeds high IQ teenagers in Israel into the upper echelons of elite Israeli military intelligence units with a focus on technology.

It is sometimes referred to as the IDF's "MENSA" and was originally created by notorious Israeli spymaster Rafi Eitan. Eitan is best known as Jonathan Pollard's handler and the mastermind behind the PROMIS software scandal, the most infamous Israeli intelligence operation conducted against Israel's supposed "ally", the United States.

Due to its focus on technological ability, many Talpiot recruits subsequently serve in Israel's Unit 8200, the signals intelligence unit of Israeli military intelligence that is often described as equivalent to the US' NSA or the UK's GCHQ, before moving into the private tech sector, including major Silicon Valley companies.

Other Talpiot-Unit 8200 figures of note are one of the co-founders of Check Point, Marius Nacht, and Assaf Rappaport, who designed major aspects of Microsoft's cloud services and later managed that division. Rappaport later came to manage much of Microsoft's research and development until his abrupt departure early last year.

In addition to his past as a Talpiot recruit and 8 years in Israeli military intelligence, the WEF's Tal Goldstein had played a key role in establishing Israel's National Cyber Bureau, now part of Israel's National Cyber Directorate, now a WEF-PAC partner. The National Cyber Bureau was established in 2013 with the explicit purpose "to build and maintain the State of Israel's national strength as an international leader in the field" of cybersecurity.

According to Goldstein's WEF biography, Goldstein led the formation of Israel's entire national cybersecurity strategy with a focus on technology, international cooperation, and economic growth.

Goldstein was thus also one of the key architects of the Israeli cybersecurity policy shift which took place in 2012, whereby intelligence operations formerly conducted "in house" by Mossad, Unit 8200 and other Israeli intelligence agencies would instead be conducted through private companies that act as fronts for those intelligence agencies.

One admitted example of such a front company is Black Cube, which was created by the Mossad to act explicitly as its "private sector" branch.

In 2019, Israeli officials involved in drafting and executing that policy openly yet anonymously admitted to the policy's existence in Israeli media reports. One of the supposed goals of the policy was to prevent countries like the US from ever boycotting Israel in any meaningful way for violations of human rights and international law by seeding prominent multinational tech companies, such as those based in Silicon Valley, with Israeli intelligence front companies.

This effort was directly facilitated by American billionaire Paul Singer, who set up Start Up Nation Central with Benjamin Netanyahu's main economic adviser and a top AIPAC official in 2012 to facilitate the incorporation of Israeli start-ups into American companies.

Goldstein's selection by the WEF as head of strategy for its cybersecurity efforts suggests that Israeli intelligence agencies, as well as Israeli military agencies focused on cybersecurity, will likely play an outsized role in WEF-PAC's efforts, particularly its ambition to create a new global governance structure for the internet.

In addition, Goldstein's past in developing a policy whereby private companies acted as conduits for intelligence operations is of obvious concern given the WEF's interest in simulating and promoting an imminent "cyber pandemic" in the wake of the COVID crisis.

Given that the WEF had simulated a scenario much like COVID prior to its onset through Event 201, having someone like Goldstein as the WEF's head of strategy for all things cyber ahead of an alleged "cyber pandemic" is cause for concern.

A Global Threat to Justify a Global "Solution"

Last November, around the same time the WEF-Carnegie report was released, the WEF-PAC produced its own "insight report" aimed at "shaping the future of cybersecurity and digital trust." Chiefly written by the WEF's Tal Goldstein alongside executives from

Microsoft, the Cyber Threat Alliance, and Fortinet, the report offers "a first step towards establishing a global architecture for cooperation" as part of a global "paradigm shift" in how cybercrime is addressed.

The foreword was authored by Jürgen Stock, the Secretary-General of INTERPOL, who had participated in last year's Cyber Polygon exercise and will also participate in this year's Cyber Polygon as well. Stock claims in the report that "a public-private partnership against cybercrime is the only way to gain an edge over cybercriminals" (emphasis added).

Not unlike the WEF-Carnegie report, Stock asserts that only by ensuring that large corporations work hand in glove with law enforcement agencies "can we effectively respond to the cybercrime threat." The report first seeks to define the threat and focuses specifically on the alleged connection between cryptocurrencies, privacy enhancing technology, and cybercrime.

It asserts that "cybercriminals abuse encryption, cryptocurrencies, anonymity services and other technologies", even though their use is hardly exclusive to criminals. The report then states that, in addition to financially motivated cybercriminals, cybercriminals also include those who use those technologies to "uphold terrorism" and "spread disinformation to destabilize governments and democracies".

While the majority of the report's discussion on the cybercrime threat focuses on ransomware, the WEF-PAC's inclusion of "disinformation" highlights the fact that the WEF and their partners view cybercriminals through a much broader lens.

This, of course, also means that the methods to combat cybercrime contained within the report could be used to target those who "spread disinformation", not just ransomware and related attacks, meaning that such "disinformation" spreaders could see their use of cryptocurrency, encryption, etc. restricted by the rules and regulations WEF-PAC seeks to promote.

However, the report promotes the use of privacy-enhancing technologies for WEF-PAC members, a clear double standard that reveals that this group sees privacy as something for the powerful and not for the general public.

This broad definition of "cybercriminal" conveniently dovetails with the Biden administration's recent "domestic terror" strategy, which similarly has a very broad definition of who is a "domestic terrorist."

The Biden administration's strategy is also not exclusive to the US, but a multinational framework that is poised to be used to censor and criminalize critics of the WEF stakeholder capitalism model as well as those deemed to hold "anti-government" and "anti-authority" viewpoints.

The WEF-PAC report, which was published several months before the US strategy, has other parallels with the new Biden administration policy, such as its call to crack down on the use of anonymity software by those deemed "cybercriminals" and calling for "international information sharing and cross-border operational cooperation," even if that cooperation is "not always aligned with existing legislative and operational frameworks."

In addition, the Biden administration's strategy concludes by noting that it is part of a broader US government effort to "restore faith" in public institutions. Similarly, the WEF-PAC report frames combatting all types of activities they define as cybercrime necessary to improving "digital trust", the lack of which is "greatly undermining the benefits of cyberspace and hindering international cyber stability efforts."

In discussing "solutions", the WEF-PAC calls for the global targeting of "infrastructures and assets" deemed to facilitate cybercrime, including those which enable ransomware "revenue streams", i.e. privacy-minded cryptocurrencies, and enable "the promotion of illegal sites and the hosting of criminal content."

In another section, it discusses seizing websites of "cybercriminals" as an attractive possibility. Given that this document includes online "disinformation" as cybercrime, this could potentially see independent media websites and the infrastructure that allows them to operate (i.e. video sharing platforms that do not censor, etc.) emerge as targets.

The report continues, stating that "in order to reduce the global impact of cybercrime and to systematically restrain cybercriminals, cybercrime must be confronted at its source by raising the cost of conducting cybercrimes, cutting the activities' profitability and deterring criminals by increasing the direct risk they face."

It then argues, unsurprisingly, that because the cybercrime threat is global in scope, it's "solution must also be a globally coordinated effort" and says the main way to achieve this involves "harnessing the private sector to work side by side with law enforcement officials."

This is very similar to the conclusions of the WEF-Carnegie report, released around the same time as the WEF-PAC report, which called for private banks to work alongside law enforcement and intelligence agencies as well as their regulators to "protect" the global financial system from cybercriminals.

The Framework for a Global Cyber Utility

This global coordination, per the WEF-PAC, should be based around a new global system uniting law enforcement agencies from around the world with cybersecurity companies, large corporations such as banks, and other "stakeholders."

The stakeholders that will make up this new entity, the structure of which will be discussed shortly, is based around 6 founding principles, several of which are significant. For example, the first principle is to "embrace a shared narrative for collective action against cybercrime."

Per the report, this principle involves the stakeholders comprising this organization having "joint ownership of a shared narrative and objective for the greater good of reducing cybercrime across all industries and globally."

The second principle involves the stakeholders basing their cooperation on "long-term strategic alignment." The fifth principle involves "ensuring value for participating in the cooperation", with such that "value" or benefit being "aligned with the public and private sectors' strategic interests."

In other words, the stakeholders of this global cyber utility will be united in their commitment to a common, public-facing "narrative" that serves their organizations' "strategic interests" over the long term.

The decision to emphasize the term "shared narrative" is important as a narrative is merely a story that does not necessarily need to reflect the truth of the situation, thus suggesting that stakeholders merely be consistent in their public statements so they all fit the agreed upon narrative.

Many organizations that are related to or are formally part of WEF-PAC are deeply invested in Central Bank Digital Currencies (CBDCs) as well as efforts to digitalize and thus more easily control nearly every sector of the global economy and to regulate the internet.

Therefore, it is reasonable to conclude that many of these groups may look to justify regulations and other measures that will advance these agendas in which they have long-term "strategic interests" through the promotion of a "shared narrative" that is deemed most palatable to the general public, but not necessarily based in fact.

Business is business, after all. The WEF-PAC report concludes with its three-tier model for "a global architecture for public-private cooperation against cybercrime."

The top level of this system is referred to as the "global partnership", which will build on the existing WEF-PAC and will "bring together international stakeholders to provide an overarching narrative and commitment to cooperate; foster interaction within a global network of entities that drive efforts to fight cybercrime; and facilitate strategic dialogues and processes aiming to support cooperation and overcome barriers in the long term."

Elsewhere in the report it notes that chief among these "barriers" are existing pieces of legislation in many countries that prohibit law enforcement agencies and government regulators from essentially fusing their operations with private sector entities, particularly those they are meant to either oversee or prosecute for wrongdoing.

In addition, the report states that this "global partnership" would focus on fostering "a shared narrative to increase commitment and affiliation", amplifying "operational cooperation" between the public and private sectors and improving "stakeholders' understanding of respective interests, needs, goals, priorities and constraints."

The second level of this system is called "permanent nodes" in the report. These are defined as "a global network of existing organizations that strive to facilitate public-private cooperation over time." The main candidates to occupy the role of "permanent nodes" are "non-profit organizations that are already spurring cooperation between private companies and law enforcement agencies," specifically the Cyber Threat Alliance and the Global Cyber Alliance.

Both are discussed in detail in the next section. Other potential "permanent nodes" mentioned in the report are INTERPOL, EURPOL and, of course, FS-ISAC. While the top level "global partnership" represents the "strategic level" of the organization, the "permanent node" level represents the "coordination level" as the nodes would supply necessary infrastructure, operational rules, and management, as well as "strategic dialogue" among member organizations.

The permanent nodes would directly enable the third level of the organization, which are referred to as "Threat Focus Cells" and are defined as representing the organization's "operational level." The WEF-PAC defines these cells as "temporary trust groups consisting of both public- and private-sector organizations and they would focus on discreet cybercrime targets or issues."

Per the report, each cell "would be led jointly by a private-sector participant, a law enforcement participant and a designated representative" of the permanent node that is sponsoring the cell.

Ideally, it states that cells should have between 10 to 15 participants and that "private-sector participants would typically represent organizations that can act to enhance cybersecurity on behalf of large constituencies, that have unique access to relevant cybersecurity information and threat intelligence, or that can contribute on an ecosystem-wide basis."

Thus, only massive corporations need apply. In addition, it states that law enforcement members of threat cells should "represent national-level agencies" or hail from "network defence or sector-specific agencies" at the national, regional or international level. Cell

activities would range from "scouting a new threat" to "an infrastructure takedown" to "arrests."

The WEF-PAC concludes by stating that "in the coming months, the Partnership against Cybercrime Working Group will continue to prepare the implementation of these concepts and widen the scope of the initiative's efforts", including by inviting "leading companies and law enforcement agencies" to pledge their commitment to the WEF-PAC's efforts.

It then states that "the suggested architecture could eventually evolve into a newly envisioned, independent Alliance to Combat Global Cybercrime." "In the interim," it continues, "the World Economic Forum and key stakeholders will work together to promote the desired processes and assess the validity of the concept."

Meet the "Nodes"

Among the organizations that the WEF-PAC highlights as shoo-in candidates for "permanent nodes" in their proposal for a global cyber utility, there are two that stand out and are worth examining in detail. They are the Cyber Threat Alliance (CTA) and the Global Cyber Alliance (GCA), both of which are formal members of the WEF-PAC.

The Cyber Threat Alliance (CTA) was initially founded by the companies Fortinet and Palo Alto Networks in May 2014, before McAfee and Symantec joined CTA as co-founders that September. Today, Fortinet and Palo Alto Networks are charter members alongside Check Point and Cisco, while Symantec and McAfee are affiliate members alongside Verizon, Sophos and Avast, among several others.

The mission of CTA is to allow for information sharing among its many partners, members, and affiliates in order to "allow the sharing of threat intelligence to better protect their customers against cyberattacks and to make the defense ecosystem more effective," according to CTA's current chief executive. CTA, per their website, also focuses on "advocacy" aimed at informing policy initiatives of governments around the world.

CTA is directly partnered with FS-ISAC and the WEF-PAC as well as the hawkish, US-based think tank the Aspen Institute, which is heavily funded by the Bill and Melinda Gates Foundation and the Carnegie Corporation.

Other partners include: MITRE Engenuity, the "tech foundation for public good" of the secretive US intelligence and military contractor MITRE; the Cyber Peace Institute, a think tank seeking "peace and justice in cyberspace" that is largely funded by Microsoft and Mastercard (both of which are WEF partners and key players in ID2020); the Cybersecurity Coalition, whose members include Palo Alto Networks, Israeli intelligence front company Cybereason, intelligence and military operative Amit Yoran's Tenable, Intel, AT&T, Google, McAfee, Microsoft, Avast and Cisco, among others; the Cybercrime Support Network, a non-profit funded by AT&T, Verizon, Google, Cisco, Comcast, Google and Microsoft, among others; and the Global Cyber Alliance, to be discussed shortly.

Another key partner is the Institute for Security and Technology (IST), which has numerous ties to the US military, particularly DARPA, and the US National Security State, including the CIA's In-Q-Tel. The CEO of the Cyber Peace Institute, Stéphane Duguin, was a participant in Cyber Polygon 2020, and the CEO of the Cybercrime Support Network, Kristin Judge, contributed to the WEF-PAC report. Some of the CTA's partners are listed in the WEF-PAC report as other potential "permanent nodes."

The CTA is led by Michael Daniel, who co-wrote the WEF-PAC report with Tal Goldstein. Daniel, immediately prior to joining CTA as its top executive in early 2017, was a Special Assistant to former President Obama and the Cybersecurity coordinator of Obama's National Security Council.

In that capacity, Daniel developed the foundations for the US government's current national cybersecurity strategy, which includes partnerships with the private sector, NGOs and foreign governments.

Daniel has stated that some of his cybersecurity views at CTA are drawn "in part on the wisdom of Henry Kissinger" and he has been an agenda contributor to the WEF since his time in the Obama administration. Daniel is one of Cyber Polygon 2021's experts and

will be speaking alongside Teresa Walsh of FS-ISAC and Craig Jones of INTERPOL on how to develop an international response to ransomware attacks.

The fact that CTA was founded by Fortinet and Palo Alto Networks is notable as both companies are intimately related. Fortinet's founder Ken Xie, who sits on CTA's board and is a founding member and advisor to the WEF's Centre for Cybersecurity, previously founded and then ran NetScreen Technologies, where Palo Alto Network's founder, Nir Zuk, worked after his earlier company OneSecure was acquired by NetScreen in 2002.

Zuk is an alumni of Israeli intelligence's Unit 8200 and was recruited directly out of that unit in 1994 by Check Point, a CTA charter member, WEF-PAC member and tech company founded by Unit 8200 alumni. Zuk has been open about maintaining close ties to the Israeli government while operating the California-based Palo Alto Networks. Fortinet, for its part, is known for hiring former US intelligence officials, including former top NSA officials.

Fortinet is a US government and US military contractor and came under scrutiny in 2016 after a whistleblower filed suit against the company for illegally selling the US military technological products that had been disguised in order to appear as American-made, but were actually made in China. Fortinet's Derek Manky is one of the co-authors of the WEF-PAC report.

Check Point's co-founder and current CEO, Gil Shwed, currently sits on CTA's board of directors and is also a WEF "Global Leader for Tomorrow", in addition to his longstanding ties to the Israeli National Security State and his past work for Unit 8200. Another Check Point top executive, Dorit Dor, is a member of the WEF Centre for Cybersecurity and a speaker at Cyber Polygon 2021, where she will speak on protecting supply chains.

Gil Shwed, over the past few weeks, has been making numerous appearances on US cable television news to warn that a "cyber pandemic" is imminent. In addition to those appearances, Shwed produced a video on June 23rd asking "Is a Cyber Pandemic Coming?", in which Shwed answers with a resounding yes.

The term "cyber pandemic" first emerged on the scene last year during WEF chairman Klaus Schwab's opening speech at the first WEF Cyber Polygon simulation and it is

notable that the WEF-connected Shwed uses the same terminology.

Schwab also stated in that speech that the comprehensive cyber attacks that would comprise this "cyber pandemic" would make the COVID-19 crisis appear to be "a small disturbance in comparison."

In addition to CTA, another international alliance named by the WEF-PAC as a "permanent node" candidate is the Global Cyber Alliance (GCA). The GCA was reportedly the idea of Manhattan District Attorney Cyrus Vance Jr. who "knew that there had to be a better way to confront the cybercrime epidemic" back in 2015.

GCA was born through discussions Vance held with William Pelgrin, former President and CEO of the Center for Internet Security (CIS) and one of New York Governor Andrew Cuomo's top cyber advisors. Pelgrin and Vance later approached Adrian Leppard, the then- police commissioner of the City of London, the controversial financial center of the UK. Unsurprisingly, CityUK, the City of London's main financial lobby group, is a member of the GCA.

If one is familiar with Cyrus Vance's time as Manhattan DA, his interest in meaningfully pursuing crime, particularly if committed by the wealthy and powerful, is laughable. Vance infamously dropped cases against and/or declined to prosecute powerful New York figures, including Donald Trump's children and Harvey Weinstein, subsequently receiving massive donations to his re-election campaigns from Trump family and Weinstein lawyers.

His office also once lobbied a New York court on behalf of intelligence-linked pedophile Jeffrey Epstein, who was seeking at the time to have his registered sex offender status downgraded.

Vance's office later U-turned in regards to Weinstein and Epstein after more and more accusers came forward and after considerable press attention was paid to their misdeeds. Vance also came under scrutiny after dropping charges against former head of the International Monetary Fund (IMF), Dominique Strauss-Kahn, for the sexual assault of a hotel maid.

Vance used $25 million in criminal asset forfeiture funds to create GCA, in addition to funding from Pelgrin's CIS and the Leppard-run City of London police. Its official yet opaque purpose is "to reduce cyber risk" on a global scale in order to create "a secure, trustworthy internet." Their means of accomplishing this purpose is equally vague as they claim to "approach this challenge by building partnerships and creating a global community that stands strong together."

For all intents and purposes, GCA is a massive organization whose members seek to create a more regulated, less anonymous internet. The role of the Center for Internet Security (CIS) in the GCA is highly significant, as CIS is the non-profit that manages key bodies involved in the maintenance of critical US infrastructure, including for US state and local governments and for federal, state and local elections.

CIS, which is also partnered with CTA, also works closely with the main groups responsible for protecting the US power grid and water supply systems and is also directly partnered with the Department of Homeland Security (DHS).

Its board of directors, in addition to William Pelgrin, includes former high-ranking military and intelligence operatives (i.e. the aforementioned Amit Yoran), former top officials at the DHS and the National Security Agency (NSA) and one of the main architects of US cyber policy under the administrations of both George W. Bush and Barack Obama.

CIS was created through private meetings between "a small group of business and government leaders" who were members of the Cosmos Club, the "private social club" of the US political and scientific elite whose members have included three presidents, a dozen Supreme Court justices and numerous Nobel Prize winners.

GCA's main funders are the founders listed above as well as the William and Flora Hewlett Foundation, the foundation of the co-founder of Hewlett-Packard (HP), a tech giant with deep ties to US intelligence; Craig Newmark Philanthropies, the "philanthropic" arm of the Craigslist founder's influence empire; and Bloomberg, the media outlet owned by billionaire and former Mayor of New York Mike Bloomberg.

GCA's premium partners, which also fund GCA and secure a seat on GCA's Strategic Advisory Committee, include Facebook, Mastercard, Microsoft, Intel, and PayPal as well as C. Hoare & Co., the UK's oldest privately owned bank and the fifth oldest bank in the world.

Other significant premium partners include the Public Interest Registry, which manages the .org domain for websites, and ICANN (the Internet Corporation for Assigned Names and Numbers), that manages much of the Internet's global Domain Name System (DNS).

Those two organizations together represent a significant portion of website domain name management globally. Notably, the founding chairwoman of ICANN was Esther Dyson, whose connections to Jeffrey Epstein and the Edge Foundation were discussed in a recent Unlimited Hangout investigation.

In terms of partners, GCA is much larger than CTA and other such alliances, most of which are themselves partners of GCA. Indeed, nearly every partner of CTA, including the CTA itself are part of the GCA as is CTA co-founder Palo Alto Networks.

GCA's partners include several international law enforcement agencies including: the National Police, National Gendarmerie and Ministry of Justice of France, the Ministry of Justice of Lagos, the Royal Canadian Mounted Police, the UK Met Police, and the US Secret Service. The state governments of Michigan and New York are also partners.

Several institutions and companies deeply tied to the US National Security State, such as Michael Chertoff's the Chertoff Group, the National Security Institute, and MITRE, are part of GCA as are some of the most controversial and intelligence-connected cybersecurity companies, such as Crowdstrike and Sepio Systems, another Unit 8200 alumni-founded company whose chairman of the board is former Mossad director Tamir Pardo.

The Israeli intelligence-linked initiative CyberNYC is also a member. Major telecommunication companies like Verizon and Virgin are represented alongside some of the world's largest banks, including Bank of America and Barclays, as well as FS-ISAC and the UK's "most powerful financial lobby", the CityUK. Also crucial is the presence of several media organizations as partners, chief among them Bloomberg.

Aside from Bloomberg and Craig Newmark Philanthropies (which funds several mainstream news outlets and "anti-fake news" initiatives), media outlets and organizations partnered with GCA include Free Press Unlimited (funded by George Soros' Open Society Foundations, the European Union, and the US, Dutch, Belgian and UK governments), the Institute for Nonprofit News (funded by Craig Newmark, Pierre Omidyar's Omidyar Network and George Soros' Open Society Foundations, among others), and Report for America (funded by Craig Newmark Philanthropies, Facebook, Google and Bloomberg).

PEN America, the well-known non-profit and literary society focused on press freedom, is also a member. PEN has become much more closely aligned with US government policy and particularly the Democratic Party in recent years, likely owing to its current CEO being Suzanne Nossel, a former deputy Assistant Secretary of State for International Organizations at the Hillary Clinton-run State Department. The many other members of GCA can all be found here.

The End of Anonymity

The considerable involvement of some of the most powerful corporations in the world from some of the most critical sectors that underpin the current economy, as well as non-profits that manage key internet, government and utility infrastructure in these organizations that comprise WEF-PAC is highly significant and also concerning for more than a few reasons.

Indeed, if all were to follow the call to form a "shared narrative", whether it is true or not, in pursuit of long-term "strategic interests", which the WEF and many of its partners directly relate to the rapid implementation of the 4th Industrial Revolution via the "Great Reset", the WEF-PAC global cyber utility could emerge sooner rather than later.

As evidenced by the architecture put forth by WEF-PAC, the power that organization would have over the public and private sectors is considerable. Such an organization, once established, could usher in long-standing efforts to both require a digital ID to

access and use the internet as well as eliminate the ability to conduct anonymous financial transactions.

Both policies would advance the overarching goal of both the WEF and many corporations and governments to usher in a new age of unprecedented surveillance of ordinary citizens.

The effort to eliminate anonymous transactions in digital currency has become very overt in some countries in recent weeks, particularly in the US. For instance, Anne Neuberger, current Deputy National Security Adviser who has **deep ties** to the US-Israel lobby, **stated on June 29** that the Biden administration was considering obtaining more "visibility" into ransomware groups' activities, particularly anonymous cryptocurrency transactions.

Such efforts could easily cross the line into state surveillance of any and all Americans' online crypto transactions, especially given the US government's history of **habitually engaging** in surveillance overreach in the post-9/11 era. One specific possibility mentioned by Neuberger was to prohibit companies from keeping crypto payments of concern secret, suggesting possible, imminent regulation of cryptocurrency exchanges.

Current efforts, per Neuberger, also include an effort to build "an international coalition" against ransomware, which will likely tie into WEF-PAC given that the FBI, DOJ and US Secret Service are already members.

Neuberger also stated that the recent public-private partnership that took down the Trickbot botnet "should be the kind of operation used to tackle ransomware gangs in the future." However, that effort, **led by WEF partner Microsoft**, preemptively took down a network of computers "out of fear that hackers could deploy [that network] to launch ransomware attacks to inhibit election-supporting IT systems" ahead of the US election.

Using Trickbot as the model for future ransomware operations means opening the door to companies like Microsoft taking preemptive action against infrastructure used by people that the government and private sector "fear" may engage in "cybercrime" at some point in the future.

Notably, on the same day as Neuberger's statements, Congressional representative Bill Foster (D-IL) told Axios that "there's significant sentiment in Congress that if you're participating in an anonymous crypto transaction that you are a de facto participant in a criminal conspiracy." Coming from Rep. Foster, this is quite significant as he is a member of the Financial Services Committee, the Blockchain Caucus and a recently formed Congressional working group on cryptocurrency.

His decision to use the phrase "anonymous crypto transaction" as opposed to a transaction linked to ransomware or criminal activity is also significant, as it suggests that the possibility that complete anonymity is seen to be the target of coming efforts to regulate the crypto space by the US Congress.

While Foster claims to oppose a "completely surveilled environment" for crypto, he qualifies that by stating that "you have to be able to unmask and potentially reverse those [crypto] transactions."

However, if this becomes government policy, it will mean the only group allowed to have complete anonymity in online financial transactions will be the State and will open the door to the government's abuse of "unmasking", which the US government has done in numerous instances over the years through the systematic abuse of FISA warrants.

It is also important to mention that the US is hardly alone in its effort to wipe out online financial anonymity in the crypto world, as several governments that are supporting Central Bank Digital Currency (CBDC) projects, which includes the US, are either moving towards or have already cracked down on the crypto space.

For example, soon after China introduced the "digital yuan", it cracked down on bitcoin miners and companies that provide services, including ads and marketing, to crypto-related entities.

This had major implications for the crypto market and resulted in a considerable reduction in bitcoin's value, which it has yet to fully recover. It is reasonable to assume that other governments will work to aggressively regulate or even ban crypto markets following the introduction of their CBDC projects in order to force widespread adoption of the digital currency favored by the State.

It is also worth highlighting the additional fact that, as China introduced the digital yuan, it also sought to crackdown on cash, stating that the anonymity offered by cash – much like anonymous crypto transactions – could also be used for "illicit activity." However, there are some obvious holes in the WEF-PAC's narratives and justifications for its "solutions."

For example, even if cryptocurrencies are banned or heavily regulated, it is unlikely that this will end cyber attacks, with hackers likely finding a new way to conduct operations that provide them with some sort of financial benefit. Cyber attacks and cybercrime precede the creation of crypto considerably and would continue even if crypto were somehow magically removed from the equation.

In addition, there has been speculation about the nature of the 3 big hacks that took place over the past year: SolarWinds, Colonial and JBS. In the case of SolarWinds, attribution of blame to "Russian hackers" came down to CIA-linked cybersecurity firm FireEye claiming that the "disciplined" methodology of the hackers could only possibly have been individuals tied to Russia's government and because FireEye's CEO received a postcard he "suspects" was Russian in origin.

Left uninvestigated was the firm Samanage, which is linked to the same intelligence networks in which the WEF's current head of cyber strategy worked for years. Regarding the Colonial pipeline hack, there is the fact that the original narrative was later proven false, as the pipeline itself remained functional, but services were halted due to the company's concerns about their ability to bill customers properly.

In addition, the US Department of Justice managed to seize the vast majority of the bitcoin ransomware payment Colonial had made, suggesting that extreme regulation of the crypto market may not actually be necessary to deter cybercriminals or recuperate ransomware payments. Surely, WEF-PAC is aware of this because the US Department of Justice is one of its members.

With the JBS hack, there is the fact that the company, the world's largest meats processor, had partnered with the WEF just months before regarding the need to reduce

meat consumption and had begun to heavily invest and acquire non-animal-based alternatives. Blackrock, a major WEF partner, is the 3rd largest shareholder in JBS.

Notably, after the hack, the situation was quickly used to warn of upcoming, widespread meat shortages, even though the disruption of the hack paused operations for just one day. In addition, the JBS hack was supposedly executed by "Russian hackers" being given "safe haven" by Russia's government.

However, JBS somehow has no problem partnering the WEF, which co-hosts Cyber Polygon alongside the cybersecurity subsidiary of Sberbank, which is majority owned by the same Russian government supposedly enabling JBS' hackers.

In addition to the effort to regulate crypto, there is also a push by WEF-partnered governments to end privacy and the potential for anonymity on the internet in general, by linking government-issued IDs to internet access. This would allow every piece of online content accessed to be surveilled, as well as every post or comment authored by each citizen, supposedly to ensure that no citizen can engage in "criminal" activity online.

This policy is part of an older effort, particularly in the US, where creating a nationwide "Driver's License for the Internet" was proposed and then piloted by the Obama administration. The European Union made a similar effort to require government-issued IDs for social media access a few years later.

The UK also launched its Verify digital ID program around the same time, something which former UK Prime Minister and WEF associate Tony Blair has been pushing aggressively to have expanded into a compulsory requirement in recent months. Then, just last month, the EU implemented a sweeping, new digital ID service that could easily be expanded to fit with the Union's past efforts to link such IDs to access to online services.

As Unlimited Hangout noted earlier this year, the infrastructure for many of these digital IDs, as well as vaccine passports, have been set up so that they are also eventually linked to financial activity and potentially online activity as well.

Ultimately, what WEF-PAC represents is a global organization that aims to neuter anonymity online, whether for financial purposes or for browsing and other activities. It is a global effort combining powerful governments and corporations that seeks to usher in a new age of surveillance that makes such surveillance a requirement to participate in the online world or use online services.

It is being sold to the public as the only way to stop a coming "pandemic" of cybercrime, a crisis taking place largely in murky parts of the internet that few understand or have any direct experience with.

Having to rely on State intelligence agencies and intelligence-linked cybersecurity firms for attribution of these crimes, it has never been easier for corrupt actors in those agencies or their partners to either manufacture or manipulate a crisis that could upend online freedom as we have known it, something these very groups have sought to implement for years.

All of this should serve as a poignant reminder that, as much as our lives have become interconnected with the internet and online activity, the fight to protect human freedom, dignity and liberty against a predatory, global oligarchy is fundamentally one that must take place in the real world, not only online. May the coming "cyber war", whatever form it takes, remind many that online activism must be accompanied by real world actions and organizing.