REPORT TO THE CISA DIRECTOR

Technical Advisory Council

High-Risk Community Protection

September 13, 2023

Introduction:

The Cybersecurity and Infrastructure Security Agency (CISA) Cybersecurity Advisory Committee (CSAC) established the Technical Advisory Council (TAC) subcommittee with the purpose of researching ways to better inform CISA's efforts with the Joint Cyber Defense Collaborative (JCDC) and its High-Risk Community Protection (HRCP) initiative.

CISA defines High-Risk Communities (HRC) as those which meet all three of the following criteria:

1. Demonstrated history of being targeted by advanced persistent threat (APT) actors.
2. Limited capacity to provide for their own defense.
3. Limited cybersecurity assistance from the United States Government (USG).

Civil society is the first community CISA is prioritizing for the HRCP initiative, but over the coming years CISA plans to expand support to other communities, such as USG employees using non-enterprise devices.

CISA's HRCP initiative, announced at the Summit for Democracy on March 30, 2023, is dedicated to strengthening the cybersecurity of high-risk communities in the United States. To start, this initiative will engage civil society organizations to learn more about the threats they are facing and how to find the support they need. Through the JCDC, CISA will lead planning efforts with key government and non-government organizations, and cybersecurity and technology companies to develop a cyber defense plan for the domestic civil society organizations which are at high-risk of being targeted by foreign state actors, or non-state groups, foreign or domestic that may seek to impede or discredit the work of civil society organizations.

While focused domestically, CISA's HRCP initiative will also contribute to the Strategic Dialogue on Cybersecurity of Civil Society under Threat of Transnational Repression, co-hosted by the United States and the United Kingdom. As part of this Strategic Dialogue, CISA and its counterparts from Australia, Canada, Denmark, Estonia, France, Japan, New Zealand, Norway, and the United Kingdom will work to improve the cybersecurity of civil society organizations, engage in information sharing on the threats facing high-risk communities, and identify opportunities for greater collaboration.

High-risk communities need to defend against common cyber threats like account takeovers, crypto miners, email scams, data leakage, and ransomware. But for organizations at high-risk of being targeted by foreign state actors, threats may also include organized online threats and harassment, espionage, and sophisticated spyware. The broad range of threats, coupled with their limited defensive capabilities, is what makes high-risk communities so vulnerable. Communities that, due to political or technical factors, consider themselves at low risk one day, might suddenly find themselves in a high-risk situation the next. For example, human rights organizations in an evolving conflict zone or a reporter who publishes an unfavorable article about a political party that then gains power.

The CISA *Shields Up: Guidance for Organizations* webpage outlines foundational principles for protecting organizations and is an effective baseline guidance for high-risk organizations. The goal of this document is to provide threat and defensive guidance, assuming these organizations are already following *Shields Up* guidance.

Currently, high-risk communities count on limited support based on the goodwill of a handful of private companies to help with securing cloud-based email accounts, provide distributed denial of service (DDoS) protection for a community's web presence, or the creation of tools to help lock down devices. Different technology companies have different sets of features to increase the level of security of targeted community members, for example, Apple's "lockdown mode" for their iPhones.

These efforts are good for the communities, but a more structured framework is needed to maximize protection at scale. For example, a structure could be coordinated such that companies already offering free services are not overly duplicating efforts and are communicating with each other to better detect threats. CISA could identify gaps and, in coordination with the protection community, could determine how to best fill them.

CISA is positioned at the intersection of high-risk communities, industry, academia, security researchers, and government. This locus grants it a powerful role in clarifying threats. For example, in helping high-risk communities determine their preliminary risk level. It also provides the opportunity to act as a facilitator in connecting these high-risk communities with security organizations and researchers, and vice-versa.

Helping members of a high-risk community to self-assess their risk level is a critical skill, and it can inform the types of protective behaviors necessary to ensure their safety. While there is no industry specific definition of what a "high" risk is, there is some consensus around factors that would constitute a high-risk. For example, a journalist organization that is reporting critically on an undemocratic state actor with a history of using malware on its opponents would be at high-risk, especially if the organization's cyber maturity and computer security resources are low.

Generally speaking, the higher the likelihood that an organization will be targeted the greater their risk. Risk can be reduced through developing and following a security program, such as the CISA *Shields Up* program, that takes into account the threats an organization faces. To illustrate this, consider the following examples of where a community would be at high-risk:

High Threat and Low Defense capacity:

High Threat: Operates in one or more non-democratic regimes, in a manner that can upset existing power structures, and the regime(s) have a history of cyberattacks, malware and harassment campaigns.

Low Defensive Capacity: No internal IT support, outdated equipment, need to use insecure channels to communicate in the country, must operate in a public manner.

An organization may be considered high-risk if they are currently the target of a harassment campaign or work within a political environment, and are underprepared to resist social engineering threats, with an underdeveloped security team that lacks a patching schedule, password management strategy, and multifactor authentication program.

As another example, if an organization works within a highly competitive environment, it may be considered high-risk because it is more likely to receive targeted spear phishing emails and calls, attempts to harass or discredit executive staff, and solicit company proprietary data with the adversary focusing on exfiltrating and leaking sensitive company data to derail competition.

It might be tempting for an under-resourced organization to decide that it is not at high-risk and therefore not much needs to be done, or to decide that in fact it is at a high-risk and so every security measure must be taken, regardless of effectiveness or cost. Regardless of what is decided, adversaries are constantly adapting and organizations will need to constantly evaluate its responses.

Once an organization has determined its threat and risk level, then it needs to take steps to safely operate at that level. From a technical perspective this could mean configuring its devices and infrastructure to operate at a higher security mode, adopting enhanced email attachment protection, moving functions to the cloud, and so on. Below is an example of the different types of advice which would be given to better protect a given device given a threat level:

Defensive posture for High-Risk Communities generally has four components:

1) Defense at the device level
    - This includes attacks against individual devices with malware, exploitation of OS or applications, and physical attacks to extract data.
2) Defense at the cloud level
    - This includes attacks against user identity such as email phishing or when combined with device attacks that use tokens or credentials to access data stored in the cloud.
3) Defense at the infrastructure or network level
    - his includes lateral movement attacks, unpatched infrastructure, misconfigured infrastructure, poor security posture management, insufficient privilege management and other systemic issues.
4) Minimize human risk
    - This includes attacks against the humans within an organization to gain access to data, money, resources, trust, access and power. Attack vectors typically include email, phone call, text message, social media, and physical threats.

The focus of this report is on technical cyberattacks and does not include threats like in-person attacks or espionage through undercover activities of a nation state. We recognize that these are threats that high-risk communities face; however, they are not explored in detail in this report. CISA can have an important role in protecting communities from offline harms.

Findings:

What communities should CISA support and in what order of priority as we grow into this mission space?

The needs of high-risk civil society vary greatly. Some organizations' primary risks are related to physical safety, intimidation, abuse, outing of members, and social engineering. Others are information related, such as spyware to reveal sources and methods, compromising accounts to impersonate people or the organization, planting false evidence, stealing money or deleting information.

Priority of support within the larger set of civil society communities is subjective; the mission of a community that is critical today may not be so tomorrow.

What is universal is the need for organizations to learn how to self-assess their risk and be able to access the tools, training, and resources to improve their security posture.

Prioritizing which communities to support and in what order requires first an understanding of which communities exist, what their missions are, which risks they face, and how CISA can best support them.

Individuals, such as Lama Fakih, Roman Gressier, and Artemis Seaford, have been targeted by nation-states with sophisticated spyware. See Appendix A for further information on these individuals. Their experiences may help CISA and its partners shape the JCDC HRCP initiative. Furthermore, by facilitating the sharing of these individuals' experiences, both in terms of gaps that led to compromise and steps taken to recover, CISA can demystify the risks and recovery steps for individuals at threat of future or under active attack.

There are numerous entities that act as hubs supporting other smaller entities within a community. For example, Internews, a 501(c)(3) non-profit, "supports independent media in 100 countries," including providing training for journalists and digital rights activists and tackling disinformation. Access Now has a free, 24/7 digital security helpline for members of civil society. The organization has previously collaborated with both Amnesty International and Citizen Lab to investigate attacks leveraging NSO Group's Pegasus spyware.

CISA has an opportunity to engage with a diverse set of high-risk civil society organizations, including ones focused on digital and human rights, reproductive rights, elections, healthcare, and journalism. CISA can better support high-risk organizations by gaining an understanding of what the organization does and how it operates, constraints such as funding, resources, support, threats to the organization and/or staff members, and what are the minimum technology communication requirements when they might need to enter "safe mode."

This type of high-risk support may benefit from a multi-faceted collaboration, including global collaboration with law enforcement and intelligence agencies. These partners can then provide technical examples of how attackers are targeting phones, laptops, social media and email to harm high-risk communities and individuals. It is essential to integrate data about hate crimes, political targeting, and counterintelligence efforts to better inform high-risk communities of what the threats are, how they operate, what to look out for, how to know they being targeted, and whom to call for help.

While the focus of this document is domestic, CISA should recognize that international high-risk communities might be using products and services based in the United States. Providing security guidance to these well-resourced and sophisticated enterprises will help improve high-risk community protection globally.

Within those communities, which type of entities should CISA support and in what order of priority? For example, should CISA focus on individuals, family members, a wide swath of non-profit organizations, or a few key force-multiplier organizations?

Prioritizing non-profit and non-government organizations (NGOs) that are already doing security enhancement work will likely be the most effective way to reach and assist in developing the cybersecurity practices of high-risk communities and the organizations that serve them. Focusing on non-profits and other entities that these communities depend on, especially those that help train and support other communities and act as hubs, will also allow CISA to achieve a greater reach with their resources.

Thus, while it is critical to ultimately help individuals and their family members, direct focus on these groups will not be as effective as working with entities in the space. Moreover, individuals within high-risk communities may be more inclined to trust and use digital security advice provided by NGOs they are already familiar with, and from NGOs who are already attuned to the communities needs and particular circumstances. Given the breadth of needs, some NGOs improving digital security in high-risk communities focus on taking a "train the trainer" approach, that will help scale efforts over a one-by-one approach.

For example, the Security Education Companion is a project to provide articles, lesson plans, and teaching materials for people teaching digital security. It was created by the Electronic Frontier Foundation and is now maintained by the Level Up network and fellow community contributors, coordinated by Simply Secure, and hosted by the EFF. The project includes practitioners from Access Now, Internews, the Library Freedom Institute, and several other organizations. Appendix B lists a set of digitally focused NGOs that will provide a useful starting point for CISA.

This type of effort allows the sophisticated NGOs in the digital security space to help keep advice and training high quality and up to date, while enabling communities with less cyber maturity to learn and then pass on those learnings to their own communities.

While "a journalist targeted by sophisticated spyware" and "healthcare worker targeted by disinformation" are both high-risk, they require different approaches for defending against the threats they are facing. A clear, focused scope will result in a solid cyber defense plan that is context-specific and actionable for these communities.

What cybersecurity harms should CISA try to address and in what order of priority?

Most broadly, the highest priority harms are those which are designed by the adversary to prevent high-risk communities and the organizations supporting them to function effectively and participate in public debates and discussions that are important to those communities. To accomplish these harms, threat actors can use direct attacks to shut down the community's online activities or key voices in the community, as well as indirect threats like information operations to discredit or misrepresent the organization or to conduct surveillance on the community to enable other attacks.

Harms are largely the result of the threat actor's intent. If the goal is to discredit an organization, then compromising and publishing data dumps, planting false evidence, and compromising key figures could be a goal. If the goal is to put the organization out of business, then ransomware and data wiper trojans, targeting of backup infrastructure, account takeover and company impersonation are all strategies. Each of these threat actors may use a variety of attack vectors, including email, call, text message, social media direct message, intelligence gathering for in person attack vectors for those at high-risk.

Focusing on spear phishing, account takeover, and spyware to track people's locations and where they live may be a good place to start to help less resourced individuals and organizations defend themselves from being misrepresented or harmed (e.g., financially, physically, or digitally).

Attacks that might specifically target individuals that make up an organization could include, personal device compromise, dumping of emails, discovering human sources, and information operations to discredit. Each attack vector has different counters, either specific technical steps that could be taken to mitigate a harm, or awareness training or changes in behavior that lowers the risk—such as encrypting a high-risk community member's laptop should it be stolen.

In determining what priority to assign to the different possible harms, the overriding priority should be the protection of life and the minimization of physical harm. To best mitigate against this threat through technical cybersecurity measures, the focus should be protecting against cyberattacks designed to gather information necessary for such in-person threats. For example, cyberattacks designed to infiltrate community members' devices and identify their contacts for later in-person attacks.

As discussed above, another important priority is preventing or mitigating attacks that are designed to undermine the effectiveness of HRC organizations or the high-risk communities themselves. The goal of attacks on civil society is often to discourage or silence opponents and critics, and remove those voices from the public discourse, making this protection a key priority for the HRC.

Secondary priorities should be on those solutions that can scale, such as tools that can be used widely, training that then can be re-taught, reports and information sharing that can be amplified by other organizations. One-off solutions or highly complex solutions, while valuable, should not be the focus at this time.

What cybersecurity offerings should CISA provide and in what order of priority?

It is difficult for HRC to assess risk and understand all of the options available to better protect themselves. Most existing resources on cybersecurity prevention and detection are focused on the broad median risk organizations who are less likely to be targeted by advanced adversaries. The tactics, tools, and procedures attackers apply to high-risk victims are commonly more specialized with an emphasis on bypassing common defenses. There is a need from the high-risk community for better guidance and tools for defending against more advanced attacks. There is no “on-ramp” from the USG for communities looking for help.

The HRC need these on-ramps to find the tutorials, tools, online training, conferences and free services offered by large cloud providers and smaller privacy focused platforms. Moreover, this on-ramp needs to be constantly updated because the threats and some of the associated security advice can change rapidly.

Existing work falls into two broad categories: advisory guidance that details general steps that organizations should take to reduce susceptibility to cyberattacks, and technical measures to resist active compromise.

Among the advisory guidance programs, one of the most well-known is *Shields Up*, which outlines principles for protecting general organizations. Other resources are listed in Appendix C.

Shields Up can be the basis for an expanded offering, making CISA an on-ramp to security measures. CISA could build on the success and visibility of the *Shields Up* guidance and expand it into a "Wizard-like"-resource that will forward organizations of sufficient risk level to further technical security recommendations.

In addition, CISA can identify gaps in mitigations and advocate for the creation of protections. One approach could be to create a “Most Wanted Mitigations" top 10 list based on real world experience of what would better protect high-risk communities, even for more specific cases such as journalism or healthcare organizations that may have specific needs and risk factors.

A *Shields Up* companion resource could be developed for post-compromise recovery (maybe "Shield Repair") that would be extremely useful. CISA could create a series of best practices and resources that civil society can use when the preventive side of this has failed, or when the civil society organization got engaged post-compromise.

These measures would be most effective if CISA ensures that the initiative has resources, staffing, and budget for the long term. For the informational materials, CISA must not just put up a website, but also have the staff and funding necessary to keep it up to date and expand as needed while working with other government and industry partners. This will give confidence to HRC and organizations in general that CISA and the USG has an enduring commitment.

Identifying simple to understand and deploy “lock down” solutions can help the largest number of people. For example, iCloud Advanced Data Protection is a security feature from Apple that disables use of iCloud from the web, a popular vector for attackers, and would help provide protection in the real-world examples of attacks in Appendix A. Among the technical measures, examples include Apple's Lockdown Mode and similar techniques for other operating systems, listed in Appendix D.

One-click lockdown tools have the added benefit of being simple to deploy and use by non-expert users, but there is no accessible list of maintained offerings and the benefits of using them. An example list of such tools is listed in the appendix to this report.

Existing efforts provide a building block for high-risk organizations to increase their security posture, but there are two limiting factors that reduce the effectiveness of these efforts. First, there is a lack of guidance regarding when an organization should deploy these measures. Second, there is no central clearing house that comprehensively surveys available resources. These factors lead not only to uncertainty (especially for low-resourced organizations without dedicated cybersecurity staff) about which security measures to undertake, which hampers the security of these individual organizations, but also to a systemic uncertainty of what mitigation gaps exist in the ecosystem, which hampers the development of mitigations to fill these gaps.

The determination of recommended mitigations can be informed by a self-reported general survey of societal/political (e.g., "Does your organization interface with oppositional media organizations abroad?") and technical (e.g., "Do individuals in your organization use their own mobile devices for organization business?") risk factors.

CISA's recommendations would draw from a CISA-maintained list of technical mitigations, such as those in Appendix C and D, and would ideally include guidance on technical mitigations directly from companies like Apple, Google, Microsoft, Meta, and other platforms/service providers. Ideally, this would mean getting buy-in from tech firms to support and enhance this effort, and CISA is perfectly positioned to be a liaison to these entities.

Offerings generally fall into two categories, the development and sharing of information resources and tools, and the participation with and coordination of other organizations already in the HRCP space.

CISA has an opportunity to become a connector, a clearing house, and a coordinator of other industry and private efforts to protect high-risk communities. By organizing workshops and gathering current best practices, CISA can create guides and online wizards to help people learn of other organizations and training that can help them.

There needs to be guidance to help HRC better understand the tradeoff between keeping all features and protections in a "default" mode for maximum compatibility, and disabling features and deploying lockdown scripts to provide enhanced protection. There are tradeoffs to be made and each HRC will need to determine for themselves what is best. Helping educate them to make an informed decision is critical.

For example, Apple says Lockdown mode is an "optional, extreme protection that's designed for the very few individuals who, because of who they are or what they do, may be personally targeted by some of the most sophisticated digital threats. Most people will never be targeted by attacks of this nature." CISA could provide guidance on how to determine who may need it.

What work already exists in this space and how can CISA be a catalyst for more investment in this work globally?

Because threats to high-risk communities are a critical security challenge, work has already been done in developing mitigations in this space. CISA needs to understand the existing work to help protect high-risk communities, as the most efficient use of CISA's resources would be to act both as a catalyst for expanding and improving the space, support and reinforce existing efforts with an enduring commitment over the long term, and guide HRC to currently available and future mitigations.

The discussions, findings and recommendations above identify both existing projects underway by civil society groups (see Question 2) and within CISA (see Question 4), which can help CISA be a catalyst.

By supporting these existing projects, and extending and expanding existing programs within CISA, CISA will be the most effective in spurring further investment in this space.

In order to make these more effective CISA should work with other internationally focused government agencies (such as the State Department's Internet Freedom program), support domestic NGOs which work with global high-risk communities, and ensure that there are sufficient resources and long-term commitment to its programs. Long term CISA commitment will give the confidence necessary for NGOs and other existing projects to further invest.

What specific actions do you think the USG can take to focus cybersecurity companies and the technology industry broadly on supporting victims?

Technology companies can continue to create features that are easier for less resourced and less technical communities to enable by default. For example, Microsoft offers "S mode", which is designed for security and performance, including exclusively running apps from the Microsoft Store. Google Chromebooks offer a simplified, and safer, experience for using their cloud services.

Targeted communities may be at a disadvantage as they may not understand all the security features of the tools they are using. Attackers have more time and resources to devote to this, with the goal of using those tools to do harm to their targets.

Less technical individuals and low resourced organizations will most likely not have the ability or resources to learn how to properly configure complex feature rich versions of existing technologies (e.g. Microsoft, Google, or Apple). Product vendors offering slimmed down secure-by-default versions of products with specific marketing to consumers and low resourced organizations could help drive those communities to using the modified versions of existing products. Alternatively, vendors could provide guidance tailored to high-risk communities for how to set up and use their platforms in the best way possible.

Recommendations:

- Engage with a diverse set of NGOs that provide support to high-risk civil society organizations. To gain a better understanding of how they support civil society, ask about:
    - What the organization does and how it operates, how it works with civil society organizations, what it offers proactively and why, what it offers reactively, the resources it's able to dedicate to this effort, constraints such as budget, resources, relationships, insight.
    - How CISA and industry partners can help support them by sharing information, connecting organizations for mutual support while promoting their efforts.
- Engage with U.S. nationals who have been targeted by nation-state actors using sophisticated spyware to learn from their experiences.
- Engage with academic researchers that study the security of individuals from high-risk communities to facilitate their interactions with and research on the needs of said high-risk communities.
- Work with the State Department's Internet Freedom program to assist them helping high-risk communities overseas.
- Define the scope of the communities and threats that CISA will focus on initially.
- Initially prioritize entities that can multiply CISA's efforts through "train the trainer" and act as trusted partners and gateways to the smaller entities.
    - Within these entities, focus on those who are serving groups which may be particularly highly targeted by governments and other threat actors.
- Prioritize the protection of life and minimize physical harms.
- Prioritize harms that can stop or undermine the effectiveness of organizations and communities' work in the public sphere.
- Prioritize preventive defense guidance to high-risk communities.
- Push out tools and how-to materials to enable low resourced organizations and individuals to evade spyware used by oppressive governments and violent organizations targeting their demographics.
- Create a high-risk reporting form online that requests certain information and shows people what to watch for and report for assistance in determining if they're being targeted and how aggressive the entity is going about targeting them.
- Identify, promote, and fund tools to help communities and organizations self-assess their cyber maturity and risk levels. For example, look to the Ford Foundation's Cybersecurity Assessment Tool as a starting point.

- Identify, promote, and fund ‘One and Done’ ways to increase protections, such as advanced protection features on phones, with explicit step-by-step instructions.
- CISA should build on the success and visibility of the *Shields Up* guidance and
    - Expand it into a "Wizard-like" resource that will forward organizations of sufficient risk level to further technical security recommendations.
    - Gather information necessary to identify mitigation gaps, and encourage the development of further mitigations.
    - Create a series of best practices and resources that civil society can use when the preventive side of this has failed, or when the civil society organization got engaged post-compromise.
- Field questions from HRC entities as they determine their risk level. CISA would fill a critical lack here, as there is a current significant gap in technical resources for such determination.
- Connect an HRC entity with a list of security vendors, open-source projects, and other resources that may be needed at that entity's risk level. This is a natural effect of CISA's positioning in between these communities.
- Connect government entities with HRC entities for the former to better understand the latter's needs and stature. As a government entity, CISA may carry enough internal weight to effectively support such conversations.
- Connect academics to HRC entities to facilitate academic studies in HRC risk management and defense. CISA's relationship with HRC entities can significantly improve the reach and applicability of academic studies on the topic and augment our understanding of risk among these communities.
- Provide threat modeling information to the HRC community to help them fully understand their threat and what is a worthwhile tradeoff for the loss of functionality for additional tech protections.
- Develop a way to provide information to HRC at an organizational level, as well as high-risk individuals directly.
- Work with partners and industry to alert HRC of detected targeting, such as what Google Gmail does when they detect a foreign adversary attempting to compromise your email account. This alert would warn the end user to move to the next level of protection, provide actionable recommendations for self-help such as revoking other linked device permissions and then signing out and back in to get a new login token.
- Provide a mechanism for people to suggest tools and guidance for CISA to review and include in their recommendations.
- Develop a life cycle to keep in touch with providers and high-risk groups to evolve these recommendations based on real world experiences.
- Continue to enable, require and push for increased security-by-default features turned on for products and devices out of the box especially for end consumers and small or low resourced user base.
- Push product vendors to consider creating slimmed down small org and non-technical user versions of their products and solutions for the end consumer, non-profit and low resourced organizations to move them off of enterprise solutions.
- Create a way to recognize companies which participate in HRC protection programs.
- Promote collaboration amongst these companies to share threat intelligence.

Appendices:

A. In-the-wild Attacks

- Victims of Candiru, Pegasus, Predator: https://github.com/GranittHQ
- FORCEDENTRY NSO Group iMessage Zero-Click Exploit Captured in the Wild - https://citizenlab.ca/2021/09/forcedentry-nso-group-imessage-zero-click-exploit-captured-in-the-wild/
- re:publica 2022: Claudio "Nex" Guarnieri: Pegasus, spyware, and our rights and freedoms - https://www.youtube.com/watch?v=DoueeVHHkOs
- When Best Practice Isn't Good Enough: Large Campaigns of Phishing Attacks in Middle East and North Africa Target Privacy-Conscious Users - https://www.amnesty.org/en/latest/research/2018/12/when-best-practice-is-not-good-enough/
- One click attack would be prevented by Lockdown mode, as it disable clicking links in Messages: https://citizenlab.ca/2016/08/million-dollar-dissident-iphone-zero-day-nso-group-uae/
- A deep dive into an NSO zero-click iMessage exploit: Remote Code Execution: https://googleprojectzero.blogspot.com/2021/12/a-deep-dive-into-nso-zero-click.html
- Exploit Archaeology: A forensic history of in-the-wild NSO group exploits: https://www.virusbulletin.com/uploads/pdf/conference/vb2022/papers/VB2022-Exploit-archaeology-a-forensic-history-of-in-the-wild-NSO-Group-exploits.pdf
- Attacks on Lama Fakih, Roman Gressier, and Artemis Seaford
  https://www.hrw.org/news/2022/01/26/human-rights-watch-among-pegasus-spyware-targets
  https://www.newyorker.com/news/news-desk/a-hacked-newsroom-brings-a-spyware-maker-to-us-court-pegasus
  https://www.nytimes.com/2023/03/20/world/europe/greece-spyware-hacking-meta.html

B. NGOs

- Citizen Lab: https://citizenlab.ca/
- Electronic Frontier Foundation: https://eff.org/
  - (Note: Mr. Kurt Opsahl is a volunteer Special Counsel with EFF)
- Security Education Companion: https://www.securityeducationcompanion.org/
- Internews https://internews.org/areas-of-expertise/global-tech/what-we-do/digital-safety/
- Access Now: https://www.accessnow.org/help/
- Freedom of Press Foundation https://freedom.press/training/
- Committee to Protect Journalists: https://cpj.org/2022/11/digital-safety-using-online-platforms-safely-as-a-journalist/
- Amnesty International: https://www.amnesty.org/
- Superbloom (Simply Secure): https://simplysecure.org/
- Global Forum on Cyber Expertise: https://thegfce.org/
- Level Up: https://level-up.cc
- Library Freedom Institute: https://libraryfreedom.org/lfi/
- Granitt: https://granitt.io/, founded by Ms. Runa Sandvik

C. Risk Management Mitigations

- Ford Foundation's Cybersecurity Assessment Tool (CAT) is designed to measure the maturity, resiliency, and strength of an organization's cybersecurity efforts: https://www.fordfoundation.org/work/our-grants/building-institutions-and-networks/cybersecurity-assessment-tool/
- CISA *Shields Up*: https://www.cisa.gov/shields-up

D. Example Lockdown Tools

- National Checklist Program: https://ncp.nist.gov/repository

- Hardentools simply reduces the attack surface on Microsoft Windows computers by disabling low-hanging fruit risky features: https://github.com/securitywithoutborders/hardentools
- Harden Windows Safely: https://github.com/HotCakeX/Harden-Windows-Security
- Microsoft Security Privileged Access: https://learn.microsoft.com/en-us/security/privileged-access-workstations/overview
- Android Advanced Protection: https://support.google.com/accounts/answer/9764949?hl=en
- GrapheneOS Mobile OS that is Android: https://grapheneos.org/
- Apple Lockdown Mode: https://support.apple.com/en-us/HT212650
- Apple Advanced Data Protection for iCloud: https://support.apple.com/en-us/HT212520
- The MacOS Hardening Project: https://github.com/ataumo/macos_hardening
- Apple configuration profiles: https://it-training.apple.com/tutorials/deployment/dm105

E. Example Posture Management Tools

- Open Cloud Security Posture Management - https://github.com/OpenCSPM/opencspm
- Scout Suite (open source) Multi-Cloud Security Posture Auditing tool https://github.com/nccgroup/ScoutSuite

F. Background Reference Documents

- Secretary Mayorkas Discusses New U.S. Efforts to Counter the Misuse of Technology and the Spread of Digital Authoritarianism at Summit for Democracy, March 30, 2023, https://www.dhs.gov/news/2023/03/30/secretary-mayorkas-discusses-new-us-efforts-counter-spread-digital-authoritarianism
- The Summit for Democracy page, March 30, 2023, https://www.state.gov/summit-for-democracy/
- JCDC Focused on Persistent Collaboration and Staying Ahead of Cyber Risk in 2023, January 26, 2023, https://www.cisa.gov/news-events/news/jcdc-focused-persistent-collaboration-and-staying-ahead-cyber-risk-2023.
- Joint Statement on the Strategic Dialogue on Cybersecurity of Civil Society Under Threat of Transnational Repression, March 30, 2023, https://www.cisa.gov/news-events/news/jcdc-focused-persistent-collaboration-and-staying-ahead-cyber-risk-2023
- CISA's *Shields Up*: Guidance for Organizations page, https://www.cisa.gov/shields-guidance-organizations

Acknowledgements

Technical Advisory Council Subcommittee Members:

Mr. Jeff Moss, Subcommittee Chair, DEF CON Communications
Mr. Dino Dai Zovi, Security Researcher
Mr. Luiz Eduardo, Aruba Threat Labs
Mr. Isiah Jones, Applied Integrated Technologies
Mr. Kurt Opsahl, Electronic Frontier Foundation
Ms. Runa Sandvik, Granitt
Mr. Steve Schmidt, Amazon
Mr. Yan Shoshitaishvili, Arizona State University
Dr. Kate Starbird, University of Washington
Ms. Rachel Tobac, SocialProof Security
Mr. David Weston, Microsoft
Mr. Bill Woodcock, Packet Clearing House
Ms. Yan Zhu, Brave Software