CYBER SECURITY & INFO TECHNOLOGIES

Cyber Civil Defense: A Path Towards Comprehensive and Coordinated Cybersecurity

APRIL 22, 2024

The rapid escalation of cyber attacks on critical infrastructure highlights an urgent need for a comprehensive approach to cybersecurity, reminiscent of the civil defense strategies developed during and after World War II. In response to the growing threats in cyberspace, the concept of Cyber Civil Defense has emerged, advocating a collective effort to protect civilians and infrastructure from cyber threats. This concept parallels historical civil defense measures, where public and civil authorities coordinated to mitigate the effects of wartime attacks through both reactive and proactive strategies, such as improvised shelters and collective dimming of lights to counter enemy bombings.

Today, as our reliance on digital technologies surges—further accelerated by the increase in remote activities during the COVID period—our societal vulnerability to cyber-attacks has exponentially grown. This vulnerability is compounded by the cyber attackers' inherent advantages, such as the ability to leverage automation and scalability, and the difficulty in attributing attacks and coordinating international efforts against cybercriminals. In 2023 alone, the US Internet Crime Complaint Center (IC3) reported a record number of complaints with significant financial losses, underscoring the critical need to enhance cybersecurity measures. Attacks targeting schools, power grids, hospitals, and other critical infrastructure have demonstrated the shortcomings of traditional perimeter security in ensuring public safety in the digital realm.

Recognizing the escalating threat, nonprofit organizations, security service providers, individual researchers, and government agencies have initiated various measures to bolster

cyber defenses. These include active vulnerability scans, dark web monitoring, incident response support, and other services aimed at preventing and mitigating cyber attacks. However, despite these efforts, a structured approach to orchestrating Cyber Civil Defense activities remains elusive.

To address this gap, there is a pressing need for a framework and a maturity model specifically tailored to Cyber Civil Defense. Such a model would enable us to understand the current state of cybersecurity efforts, identify critical gaps, and determine the next steps for enhancing the resilience of individuals and organizations against cyber threats. It would answer key questions about the coordination of Cyber Civil Defense activities, the capabilities and resources currently available, and the prioritization and provision of these resources to various stakeholders, from individuals to large corporations.

The development of a Cyber Civil Defense Maturity Model is essential to efficiently orchestrate the myriad efforts underway and ensure that cybersecurity measures are accessible and effective across different levels of society. This model will serve as a foundational step in advancing our collective cybersecurity posture, thus reducing the adverse effects of cyber attacks on civilians and safeguarding access to essential human rights in an increasingly digitized world.

CURRENT LANDSCAPE

Currently, Craig Newmark Philanthropies leads the Cyber Civil Defense concept; moreover, government entities, non-profit organizations, security providers, and individuals creating open-source projects are working to provide different resources and services to address the security needs of individuals and organizations.

To capture a snapshot of the current situation, we can evaluate the following organizations that are well-known in their fields and used by many institutions and individuals. This is not an exhaustive list of current Cyber Civil Defense providers but is shared only to serve as examples in their respective fields.

- **– Government agencies:** The Cybersecurity and Infrastructure Security Agency (CISA), the Federal Bureau of Investigation(FBI), and the US Secret Service.
- **– Non-profit organizations:** The Shadowserver Foundation, Security for Community, Quad9, The Cyber Helpline, and Global Resiliency Federation (GRF).
- **– Security providers:** Qualys and SOCRadar Cyber Intelligence.
- **– Open-source project:** Wazuh, Velociraptor, and Vigil.

Government agencies may provide different security services to individuals and companies such as fraud prevention or incident response. These services can create value for a specific industry, country, or the globe generally. They include the following:

– The **Secret Service** supports cyber investigations to protect the US's financial infrastructure. The Cyber Fraud Task Force, for example, provides services to prevent, detect, and mitigate complex cyber-enabled financial crimes. Additionally, it provides support for transnational cybercrime investigations.

– The **FBI** is the lead federal agency to investigate cyber attacks and intrusions. Victims report incidents to the Internet Crime Complaint Center (IC3), and the FBI starts investigations and incident response activities.

– **CISA** provides security services for critical US infrastructures, including scanning their digital infrastructure to detect Known Exploitable Vulnerabilities (KEV), among other capacity-building efforts.

Nonprofit cybersecurity organizations can cover a group or region but also provide services on a global scale.

– **The Shadowserver Foundation** provides vulnerability scanning to detect critical vulnerabilities of organizations to prevent cyber attacks globally. They offer free services to any organization.

– **Security for Community** conducts dark web research and globally provides free victim notification services for any individual and company. These notifications enable victims to take action to prevent further attacks targeting them or the organizations they work for.

– **Quad9** provides a free secure DNS service globally. They receive threat feeds from threat intelligence companies and block user requests from reaching malicious resources.

– **The Cyber Helpline** provides expert help for victims of cybercrime, digital fraud, and online harm in the UK and the US.

– **GRF** creates industry-based information-sharing communities to distribute threat information to prevent cyberattacks. Financial Services Information Sharing and Analysis Center (**FS-ISAC**), **Manufacturing ISAC**, K12 Security Information eXchange (**K12SIX)**, and **Healthcare ISAC** are some of them.

Some **for-profit cybersecurity providers** also provide free services to benefit the community and support Cyber Civil Defense activities. Important examples include the following:

– **Qualys** provides free active scanning capabilities globally to discover IT assets, manage vulnerabilities, scan web applications, and perform inventory cloud assets.

– **SOCRadar Cyber Intelligence** offers a free cyber-threat intelligence tool that enables threat hunting and malware analysis capabilities for any security team globally. It provides resources for researching vulnerabilities, threat actors, malware, and threat feeds, and offers dark web visibility.

In some cases, individual security researchers work on **open-source projects** to create security tools to support the community in their Cyber Civil Defense activities. Some examples include the following:

– **Wazuh**, as an open-source Extended Detection and Response (XDR) and Security Information and Event Management (SIEM) tool, provides threat detection, prevention, and response capabilities. It can be used globally by any entity.

– **Velociraptor**, as an open-source digital forensics and incident response tool, supports its users in conducting sophisticated digital forensics activities and reduces the burden on security professionals by providing automation and scalability.

– **Vigil**, as an open-source Large Language Model (LLM) security scanner, enables its users to detect prompt injections, jailbreaks, and other potential threats.

For institutions to benefit more efficiently from Cyber Civil Defense activities, some institutions and individuals list the most popular resources and share them with their followers. CISA shares free tools approved for critical infrastructures, and other nonprofit organizations like Global Cyber Alliance bring together nonprofit cybersecurity organizations. However, these activities highlight only a limited number of firms operating in the Cyber Civil Defense field.

For an individual or an SMB, there are unfortunately no comprehensive sources to answer questions like: “What kind of support do I need in which areas, and how can I obtain it? What capability gaps do I have with the security products I currently have?”

Similarly, if security professionals, individuals, or institutions want to donate to the Cyber Civil Defense field, there are insufficient resources to answer questions about existing area needs and the type of services donors can provide to create more added value.

In evaluating the current landscape, it is evident that there is a need for an inclusive resource to make current Cyber Civil Defense activities more accessible to more people and institutions and to manage Cyber Civil Defense activities more inclusively and efficiently.

HOW TO USE THE MATURITY MODEL

Different entities may use the maturity model from different perspectives. It is of use to an enterprise, an entity that wants to financially support cyber civil defense activities, or a security researcher who wants to contribute, as the following examples demonstrate:

– A mid-sized energy-distribution company from Kentucky may check the Cyber Civil Defense Maturity Model to learn what kind of free and paid cybersecurity resources are globally available for a US-based energy company. After that, they may utilize some of the resources and understand which type of services/products they should get first.

– An individual from California who wants to support the community for Cyber Civil Defense activities but does not know where to invest money, what the current gaps are, and which areas could use resources to create more value may check the Cyber Civil Defense Maturity

Model to address these questions. After realizing the gaps, the individual may choose to support local or global efforts in the needed domains.

– A cyber-threat intelligence analyst who wants to contribute to the security of the community may check the Cyber Civil Defense Maturity Model to understand available resources and gaps. After reviewing the current resources and gaps, our analyst may choose to contribute to one of those nonprofits listed in the maturity model or create a new organization to address the needs.

These are the main use cases and some examples of how to use the Cyber Civil Defense Maturity Model, but they are not limited to the ones listed here. Having that big picture may create value for different entities from different domains.

FUNDAMENTALS FOR THE REQUIRED FRAMEWORK

Individuals and institutions are exposed to different types of cyber attacks due to the different infrastructures they use. Therefore, their need to prevent attacks varies. For Cyber Civil Defense activities to be managed more inclusively and efficiently and for more people and institutions to benefit from them efficiently, the frameworks required must fundamentally have the following features

Since organizations providing Cyber Civil Defense have different solutions in this context, **separate frameworks need to be created for individuals and institutions**.

Cybersecurity can be provided by utilizing **different types of strategies**. So that the gaps in cybersecurity measures are clearly understood, the Cyber Civil Defense maturity model should include the following strategies:

– **Proactive strategies** aim to prevent cyber threats by preparing for them and fortifying them in advance.

– **Active strategies** involve ongoing efforts to detect and neutralize threats as they occur.

– **Reactive strategies** focus on efficiently responding to and recovering from cyber incidents and analyzing them to prevent future occurrences.

Cybersecurity measures have **different aspects**, each one with different qualifications.

– **Prevention**: Implementing measures to stop cyberattacks before they occur.

– **Detection**: Identifying security threats and breaches as early as possible.

– **Response**: Taking immediate action to contain and neutralize detected threats.

– **Recovery**: Restoring systems and operations to normal after a security incident.

– **Mitigation**: Reducing the impact or severity of an incident by taking corrective steps.

– **Adaptation**: Adjusting strategies and practices in response to evolving cyber threats.

To improve the Cyber Civil Defense Maturity Model, the above aspects of cybersecurity should be included in the framework.

Some organizations focus more on providing services in specific countries, like national CERTs or nonprofit organizations. To better understand the gaps and ensure that the necessary services can be provided in different regions, **the country factor should also be included** in the Cyber Civil Defense framework. Concurrently, of course, global resource providers should be considered and analyzed at a level that also allows for local analysis. For instance, a person in the United States can receive breached credential services from the **Australia-based HaveIBeenPwned**, secure DNS service from the **Switzerland-based Quad9**, or victim support services from **the UK-based Cyber Helpline**. Therefore, resources should be evaluated globally.

Some industries may have specific cyber risks, and to address them, other organizations may provide specific services. It is also common to see that organizations in the same industries come together to share intelligence and provide a collective cybersecurity approach. Therefore, the sources of Cyber Civil Defense **should also be analyzed by industry**.

Cyber Civil Defense resources may include free or low-cost cybersecurity services, training, and products. Entities in need should be able to choose from free resources or invest in low-cost alternatives. A better approach would **consider enterprise-level solutions** to provide more alternatives to individuals and companies.

A Cyber Civil Defense maturity model should include **resources from different entities** to be more comprehensive and usable. The resources created by government entities, nonprofit organizations, for-profit businesses, and open-source projects should be included in the framework.

For individual and corporate needs to be addressed more efficiently, cybersecurity services grouped by **strategy and aspect should be weighted according to their importance**. With this weighting, institutions will be able to correctly prioritize the steps they need to take, and cybersecurity professionals and sponsors in this field will also find the opportunity to make more accurate investments.

Organizing Cyber Civil Defense activities according to strategy, aspect, country, sector, cost, source, importance, and priority separately for individuals and institutions, alongside evaluating the maturity level of Cyber Civil Defense activities, can create benefits by setting a target for individuals and institutions.

CONCLUSION

The increase in the number and impact of cyber attacks on society and its institutions has reached dimensions that cannot be met solely with public resources. The need for measures to be taken within the scope of public safety makes it inevitable that the concept of civil defense, which civilians had to implement after WWII, be applied today as Cyber Civil Defense.

Currently, government entities, non-profit organizations, security providers, and individual security researchers have started to act within the scope of Cyber Civil Defense. However, for these activities to be efficiently supported by different entities, a big picture and a maturity model must be provided.

Correspondingly, the maturity model outlined above, addressing the fundamental issues, should be developed for individuals and institutions. This way, institutions, individuals, and security researchers can increasingly contribute to and benefit from Cyber Civil Defense.

Orion Policy Institute (OPI) is an independent, non-profit, tax-exempt think tank focusing on a broad range of issues at the local, national, and global levels. OPI does not take institutional policy positions. Accordingly, all views, positions, and conclusions represented herein should be understood to be solely those of the author(s) and do not necessarily reflect the views of OPI.