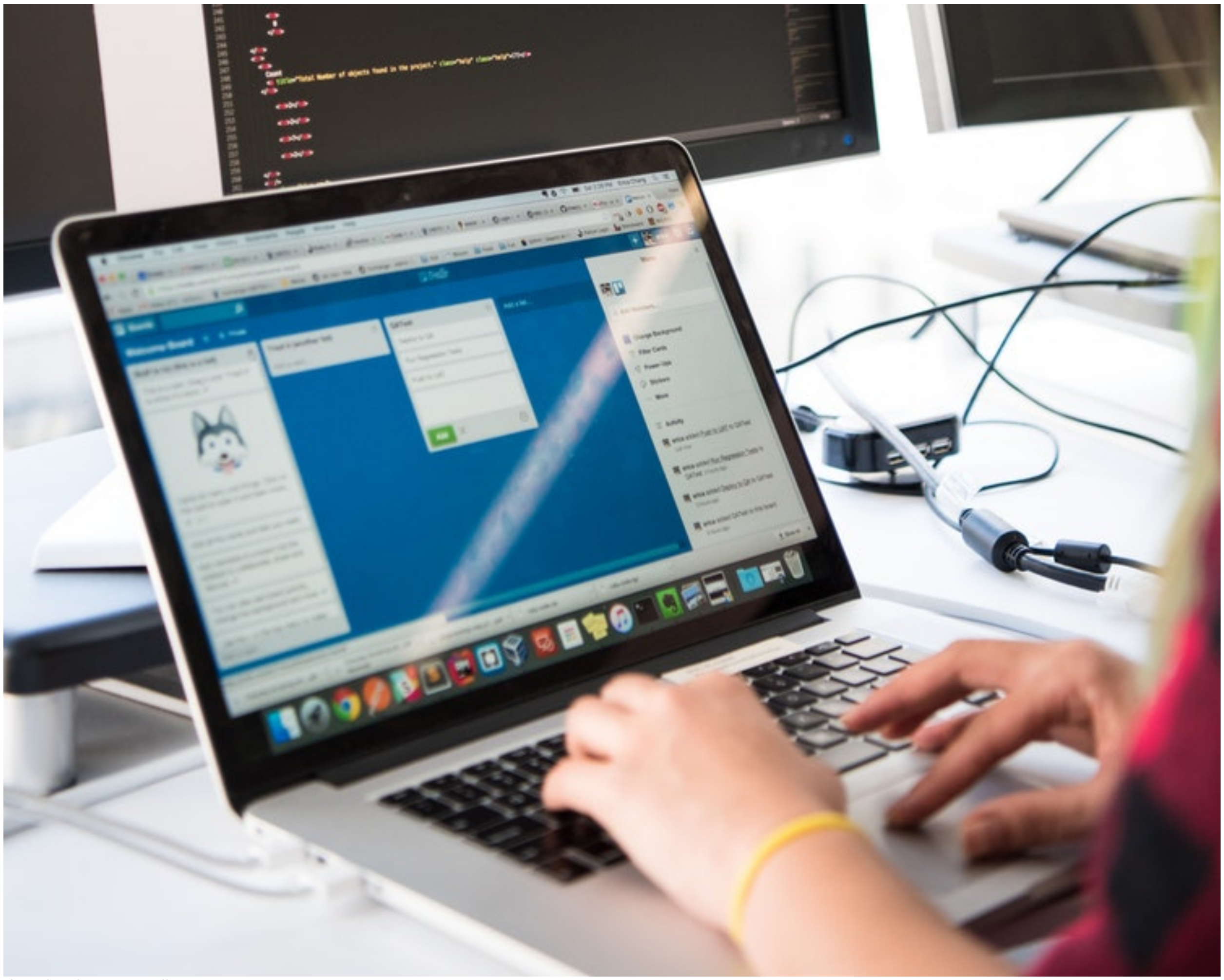


Photo by Christina Morillo

Helping Cities Respond When A Cyber-Attack Strikes

How to Leverage Cyber and Technology Professionals as Volunteers During a Response

May 2020

COLUMBIA | SIPA
School of International and Public Affairs

NYC
Cyber Command

ACKNOWLEDGMENTS

Helping Cities Respond when a Cyber-Attack Strikes:
Leveraging Cyber and Technology Professionals as Volunteers During a Response

Faculty Advisor: Katheryn Rosen

Co-Authored By:

Ray Herras

Jack Janson

Takayuki Miyazaki

Marie Natsvlishvili

Shenhav Ruttner

Yushan Xu

Impact of COVID-19 Pandemic

As a result of the 2020 COVID-19 Pandemic, which included the closure of Columbia University's campus and widespread social distancing, our Capstone team was forced to adapt to an online and virtual approach consistent with Federal and State social distancing guidelines and recommendations. Subsequently, the following report reflects diminished access to otherwise occupied emergency management personnel and other germane experts, which may have allowed our team to make more informed and prescriptive recommendations relating to the creation of a volunteer cyber corps for New York City.

GLOSSARY

ANSI	American National Standards Institute
CERT	Community Emergency Response Team
CLC	Cybersecurity Life Cycle
DoDD	United States Department of Defense Directive
DMAT	Disaster Medical Assistance Team
DoITT	New York City Department of Information Technology and Telecommunications
DTMB	Michigan State Department of Technology, Management and Budget
EDL CDU	Estonian Defence League Cyber Defence Unit
EMS	Emergency Medical Service
ERVC	Emergency Response Volunteer Corps
FASNY	Firemen's Association of the State of New York
FEMA	United States Federal Emergency Management Agency
FSVC	Financial Services Volunteer Corps
ITS	New York State Office of Information Technology Services
MiC3	Michigan Cyber Civilian Corps
MSP	Michigan State Police
NDA	Non-Disclosure Agreement
NICE	NIST National Initiative for Cybersecurity Education
NIST	United States National Institute of Standards and Technology
NYC	New York City
NYC3	New York City Cyber Command
NYPD	New York Police Department
OC3	Ohio Cyber Collaboration Committee
OEM	New York City Office of Emergency Management
OhCR	Ohio Cyber Reserve
ONG	Ohio National Guard
SIPA	Columbia University School of International and Public Affairs
USFA	United States Fire Administration
VOAD	Voluntary Organizations Active in Disaster
VPA	United States Volunteer Protection Act of 1997

TABLE OF CONTENTS

Executive Summary 5

Methodology 6

Understanding the Role of NYC3 7

About New York City Cyber Command (NYC3) 7

Volunteer Inclusion & Organizational Preparedness 9

Case Studies 11

Cybersecurity Volunteer Models 11

Michigan Cyber Civilian Corps (MiC3) 12

Ohio Cyber Reserve (OhCR) 16

Estonian Defence League Cyber Defence Unit (EDL CDU) 19

Non-Cybersecurity Volunteer Models 24

Operationalization: Hurricane Sandy 24

Recruitment & Retention: Firefighters and EMS 28

Industry Engagement: New York State COVID-19 SWAT Team 30

Effective Use of Highly Specialized Experts: Financial Services 31

Legal Considerations 34

Defining a Maturity Model for Cyber Volunteer Structures 37

Key Findings & Recommendations 43

Appendix 47

EXECUTIVE SUMMARY

New York City Cyber Command (NYC3), as the city agency tasked with protecting New York City's systems and directing citywide cyber incident response, is committed to ensuring the City remains safeguarded against all manner of cyber threats. NYC3's mission has become critical, as cybersecurity has become one of the foremost priorities for private enterprise and public institutions. However, despite a multitude of new approaches to mitigate cyber risk, the reality is apparent. Most locales in the U.S. and abroad simply lack enough resources to respond and recover from large scale cyber events on their own, especially in times of crisis. NYC3 has sought the help of a graduate Capstone team from Columbia University's School of International and Public Affairs (SIPA) to (1) study designs for a volunteer cyber auxiliary corps with the capability to augment NYC3's cyber incident response and (2) articulate a maturity model for such volunteer programs.

Our research examined existing volunteer models and codified state and national programs in both cybersecurity and non-cybersecurity contexts, such as cyber frameworks developed in the State of Michigan and Estonia and domestic volunteer firefighter organizations. This brought forth questions of legal liability in the absence of legislation that specifically protects cyber volunteers, such as a cyber-specific "good samaritan" law when they're called to act in specific phases of the cybersecurity life cycle. Building on findings made through our case study approach, our Capstone team subsequently developed a maturity model designed to assess the sophistication of a volunteer corps along eight parameters. The maturity model provided, alongside the following recommendations, serves as a tool that can be used to inform NYC3's next steps in moving forward with the formation of a cyber volunteer corps.

Key Recommendations

- **Define the scope of NYC3's volunteer cyber corps**. NYC3 should conduct an organizational needs assessment as a foundational tool for the establishment of a volunteer cyber corps.
- **Solidify volunteer framework and design.** A dedicated volunteer management staff is needed for NYC3 to develop a systematic approach to volunteer engagement and inclusion as well as managing on-going lines of communication.
- **Create an approach to volunteer engagement and outreach.** NYC3 ought to initiate an engagement strategy that includes a detailed qualifications screening process, outlines available volunteer pools, and explores incentives to drive participation.
- **Address remaining legal considerations for both NYC3 and its volunteers.** Given the nature of cybersecurity volunteer work, ensuring that volunteers have adequate legal protection is key to driving robust volunteer participation and overall program effectiveness. Supporting legal codification, e.g. of a cyber-specific "good samaritan" law, could shield volunteers from potential liability issues.

METHODOLOGY

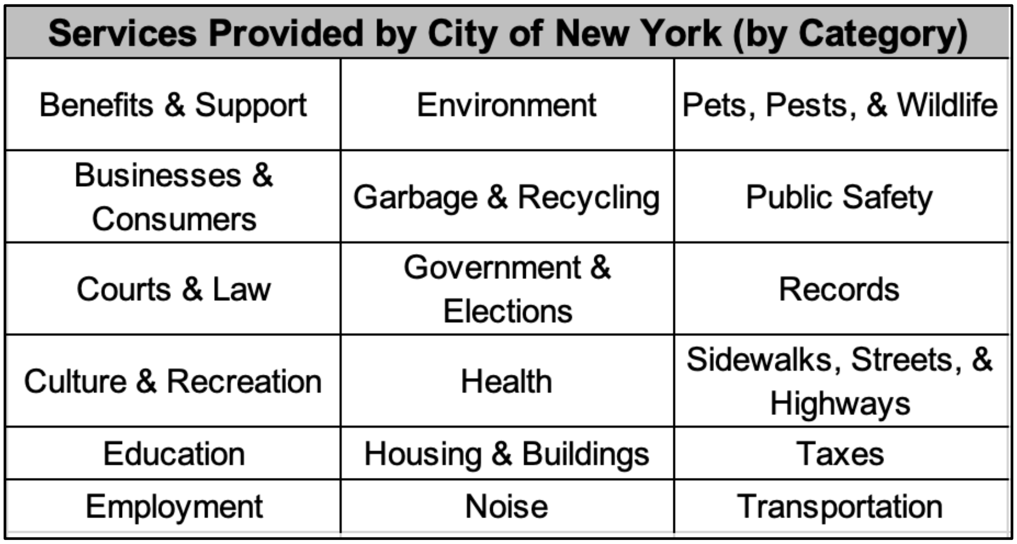
To examine the questions NYC3 asked SIPA to explore, our Capstone team first sought to develop an understanding of NYC3's organizational capacity. Second, we wanted to gain insight into what motivates volunteers to participate in programs in times of crisis and blue-sky days. Next, taking into consideration volunteerism and our familiarity with NYC3, our team conducted additional research on a case-by-case basis of existing cyber and non-cyber volunteer programs to understand existing models and how they may lend themselves to New York City's municipal structure and deep pool of available talented resources. This approach was centered around conducting an extensive series of interviews with individuals that participate in existing programs, such as Michigan's Cyber Civilian Corps (MiC3) and those from private industry with robust cybersecurity practices in place, including individuals who conduct cybersecurity operations in the financial sector.

UNDERSTANDING THE ROLE OF NYC3

About New York City Cyber Command (NYC3)

Established by Mayor Bill DeBlasio through New York City (NYC) Executive Order 28 in 2017, NYC3 is a growing and evolving organization with big responsibilities in its cyber defense mission: to lead the City of New York's cyber defense and response efforts, including the protection of agency systems, essential services, critical infrastructure and public-facing websites linked to information systems, for the largest city in the United States.[1] NYC3's additional responsibilities, executed in collaboration with the NYC Department of Information Technology and Telecommunications (DoITT), include: create and enforce information security policies and standard, execute citywide cyber incident response and cyber defense; and, advise the Mayor and Deputy Mayor on cyber defense and information risks to the City and its agencies.[2]

In all, NYC3 serves more than 100 departments and offices spread across the City of New York. The cyber defenses provided by NYC3 are critical to ensure City services (Table 1) reach its residents in a highly available and secure manner.



Services Provided by City of New York (by Category)		
Benefits & Support	Environment	Pets, Pests, & Wildlife
Businesses & Consumers	Garbage & Recycling	Public Safety
Courts & Law	Government & Elections	Records
Culture & Recreation	Health	Sidewalks, Streets, & Highways
Education	Housing & Buildings	Taxes
Employment	Noise	Transportation

Table 1. Categories of City of New York Government Services [3]

NYC3's broad cybersecurity mandate covers the Cybersecurity Life Cycle (CLC) of Identify, Protect, Detect, Respond, and Recover. In addition to protecting the City's systems, NYC3 desires to bring cyber defense and awareness to a city population of

[1] The City of New York Office of The Mayor Executive Order No. 28. July 11, 2017. https://www1.nyc.gov/assets/home/downloads/pdf/executive-orders/2017/eo_28.pdf

[2] Ibid.

[3] "Categories Page." New York City Government Website. Accessed 21 April 2020. https://www1.nyc.gov/nyc-resources/categories.page.

nearly 9 million people. New York is the only municipality that we are aware of that has set out to tackle such a comprehensive mandate in cybersecurity.

In pursuit of its mandate, NYC3's operational capacities can be illustrated by three key areas related to cyber defense and incident response[4]:

- **Threat Management**
  - 24/7 Security Operations Center
  - Oversee Incident Response
  - Gather Cyber Threat Intelligence
- **Security Sciences**
  - Focus on Employing City Cyber Defense Technology
  - Conduct Cyber Projects and Software Development
  - Support Data Science Initiatives and Cybersecurity Engineering
- **Urban Technology**
  - Smart Cities Program and Cross Collaboration
  - Utilization of Critical City Infrastructure
  - New Technology (e.g. Next Generation 911 Systems)

[4] Leadership, https://www1.nyc.gov/site/cyber/about/nyc-cyber-command-leadership.page

VOLUNTEER INCLUSION & ORGANIZATIONAL PREPAREDNESS

History proves that when disaster strikes, New Yorkers respond. They work tirelessly to help each other, and the City recover. Whether it is a devastating hurricane or a public health event, the City has tremendous success leveraging the professional expertise of New Yorkers as volunteers in a city-wide response. Before delving deeper into different aspects of forming a cyber volunteer corps, it is first important to outline the benefits or incentives for both NYC3 and its volunteers.

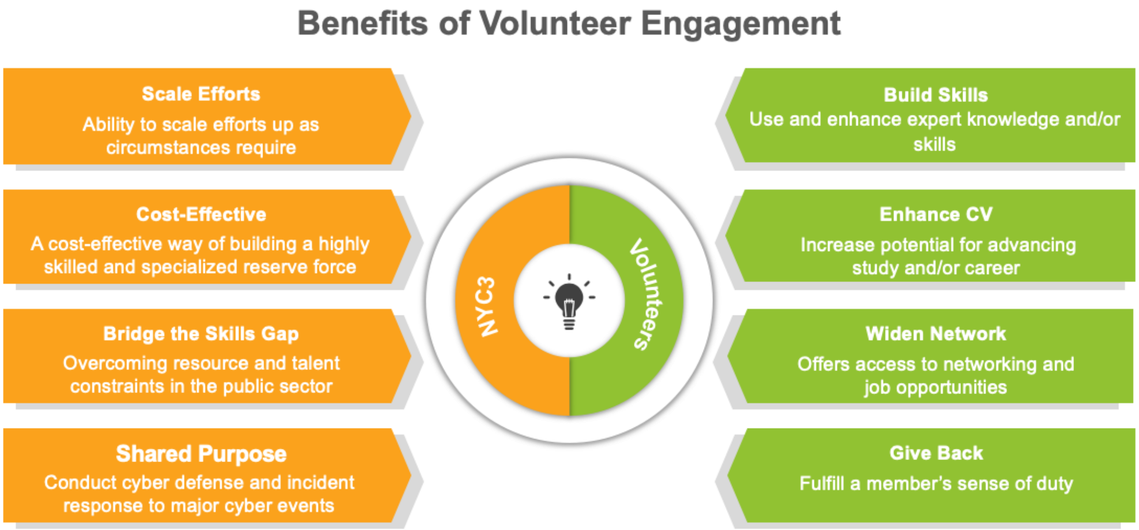

Benefits of Volunteer Engagement
Scale Efforts
Ability to scale efforts up as circumstances require
Cost-Effective
A cost-effective way of building a highly skilled and specialized reserve force
Bridge the Skills Gap
Overcoming resource and talent constraints in the public sector
Shared Purpose
Conduct cyber defense and incident response to major cyber events
NYC3
Volunteers
Build Skills
Use and enhance expert knowledge and/or skills
Enhance CV
Increase potential for advancing study and/or career
Widen Network
Offers access to networking and job opportunities
Give Back
Fulfill a member's sense of duty

Figure 2. Benefits of NYC3 Volunteer Engagement[5]

Cyber incidents present a unique challenge and require new approaches to leverage professional expertise throughout the cyber life cycle, especially as hiring and retaining IT staff can be a challenge in the public sector. This is due to public sector salaries generally not matching those in the private industry.[6] Considering this, based on our research and interviews conducted, we have summarized a list of benefits [7] that NYC3 could ensure by recruiting civilian cyber volunteers. These benefits include:

- Giving NYC3 a new pool of cybersecurity talent to enhance its response capacity during significant cyber-attacks;
- Taking care of the many low-sensitivity tasks necessary to get city services up and running again, freeing up city IT staff for higher-value work;

[5] Drawn by SIPA Capstone Project Team based on research and interviews.
[6] "*Fighting Cyberattacks With Volunteers*," Jenni Bergal, August 2, 2017, https://www.huffpost.com/entry/fighting-cyberattacks-with-volunteers_b_597f4390e4b0c69ef70529c0.
[7] Caroline Williams, "*The Impact of Volunteering in Archives*," March 2018, http://www.archives.org.uk/images/Volunteering/Williams_The_Impact_of_Volunteering_in_Archives_2018.pdf

- Giving NYC3 hands-on expertise and consultation when unique cyber threat strikes;
- Acting together to achieve a shared purpose.

On the other hand, in the process of designing its volunteer program, NYC3 should be aware of the needs that cybersecurity professionals have. Based on the interviews with current and prospective volunteers we have summarized key factors that drive volunteers to participate in a cyber volunteer corps:

- A strong sense of duty and giving back to their community;
- Continuing professional and skills development;
- Access to training that might not be otherwise available;
- Networking opportunities.

As NYC3 considers building a volunteer corps, there are additional behavioral considerations when engaging cyber professionals, among other factors: alleviating the burdens of paperwork for volunteer responders; management of time demands; developing a clear mission statement for the volunteer cyber corps; clarification of volunteer roles and responsibilities; participatory management; and effective internal communication mechanisms.

CASE STUDIES

To build the foundation for our cyber volunteer corps maturity model and recommend designs for NYC3's volunteer framework, we researched a number of existing cybersecurity and non-cybersecurity volunteer programs, both in the U.S. and abroad. In this chapter, we first examine three prominent cybersecurity volunteer models whose main mission areas include cyber incident response and analyze key components of the programs, such as mission statement, legal foundation, and organizational management. We then look into four selected non-cybersecurity volunteer cases, each of which provides good practices and lessons applicable for NYC3's volunteer framework, from the perspectives of emergency response, engagement in highly demanding roles, public-private partnership, and effective use of professional expertise.

Cybersecurity Volunteer Models

For our initial scope of research, we explored programs such as the Wisconsin Cyber Response Teams, Marine Cyber Volunteer Auxiliary, and the Cyber Specialists and Cyber Volunteers Program in the UK. However, after analyzing the context surrounding each program, our Capstone team chose cases that meet the following criteria: 1) programs that should be able to augment the cybersecurity workforce; 2) incident response is included in their scope and mission, and 3) programs that aim to serve a wide range of entities. However, we did not find evidence of municipal-level programs that satisfy these criteria, in the U.S. nor internationally. As such, we determined that the Michigan Cyber Civilian Corps (MiC3), the Ohio Cyber Reserve (OhCR), and the Estonian Defence League Cyber Defence Unit (EDL CDU) are the most relevant volunteer programs that warrant deeper analysis. We based our study on the legal and foundational documents of each program, reports published by academic institutions, interviews with management and members of the aforementioned programs, and official press releases and guidelines.

Additionally, the following programs were evaluated based on the following attributes:

- Augmentation needs and mission;
- Supporting legal framework;
- Membership requirements;
- Operational details and deployment;
- Challenges.

Michigan Cyber Civilian Corps (MiC3)

Michigan State Governor Rick Snyder announced the formation of a cyber civilian corps in 2013, and the state began to assemble a group of information security professionals. It started as a joint effort between the Department of Technology, Management and Budget (DTMB) with Merit Networks.[8] For more effective management, the operational responsibility of the MiC3 (Michigan Cyber Civilian Corps) was later transferred from Merit to the DTMB. The MiC3 is the first state-level cybersecurity volunteer corps program in the U.S. Today, the MiC3 has over 100 civilian members from local companies, universities, and civil society that work closely with the Michigan Army, Air National Guard, and the Michigan State Police (MSP).[9]

Augmentation Needs & Mission Analysis

The state of Michigan recognized a gap in the cyber incident response capabilities of many small governmental and private entities across the state. To address that problem, the mission of the MiC3 has been set to provide rapid response assistance to all levels of government, education, nonprofit, and business organizations in the State of Michigan in the event of a cyber incident.[10]

Legal Framework

Although the proposal and preparation to officially launch the MiC3 occurred in 2013, state-Level Legislation was needed to grant legal recognition and operational authorization to the MiC3. Public Act 132 of 2017 (Cyber Civilian Corps Act) was signed into law 4 years later by Governor Snyder. Subsequently, the MiC3 is administered by the DTMB, Cybersecurity, and Infrastructure Protection.[11] As for individual legal status, members of the MiC3 are not agents, employees, or independent contractors of Michigan State for any purpose.[12]

[8] Interview with a volunteer coordinator from the Michigan Cyber Civilian Corps (MiC3).

[9] "*Bridging State-level Cybersecurity Resources*," Monica M. Ruiz, October 23, 2018, https://www.lawfareblog.com/bridging-state-level-cybersecurity-resources.

[10] "*Michigan Cyber Civilian Corps*," Michigan State Government Website, accessed April 19, 2020, https://www.michigan.gov/som/0,4669,7-192-78403_78404_78419---,00.html.

[11] State of Michigan Office of the Auditor General, "*Performance Audit Report - Michigan Cyber Civilian Corps*," September 2019, https://audgen.michigan.gov/wp-content/uploads/2019/09/r071051919-0007.pdf.

[12] State of Michigan Act 132 of 2017, January 24, 2018, http://www.legislature.mi.gov/(S(aexktz02js5cm0xw0b33ginn))/documents/mcl/pdf/mcl-Act-132-of-2017.pdf.

Membership

Admittance Requirements and Steps

The MiC3 requires individuals interested in joining to have a minimum of two years of direct involvement with information security, preferably security operations and incident response. They must also possess at least one necessary security certification, with ANSI-certified/DoDD 8570-compliant certifications preferred.[13] Applicants who pass the primary screening will receive five tests, covering Basic Security, Beginning and Advanced Incident Response, and Beginning and Advanced Forensics. They have to pass four of them to be qualified. After the application, the DTMB requires the MSP to conduct a criminal history check on the individual and a criminal record check through the Federal Bureau of Investigation on the Individual.[14]

Applicants receiving invitations to join the MiC3 will have to enter into a volunteer contract with the DTMB. The contract includes provisions acknowledging the confidential information and requires the volunteer to avoid conflicts of interest and to comply with all existing department security policies and procedures. It is not an employment contract but more like a certificate of their contribution to the state and serves as a communication tool with the employers of the volunteers.[15]

Training

MiC3 members are eligible to receive state-funded cybersecurity training with a selection of courses from SANS, including SEC 504, SEC511, and FOR 572. The contents of the courses cover incident handling, security operations, network forensics, and other topics that are essential for cybersecurity.[16] Interviews revealed that these courses are of great value to MiC3 members. Training has been a great incentive for the members of MiC3 because it enhances their professional skills as well as serving as a networking platform.

Legal Protection

In addition to the volunteer contract that MiC3 volunteers sign with the DTMB, there are specific legal protections for cyber volunteers in Michigan. MiC3 volunteers are given immunity from liability or claims of negligence within the scope of the MiC3 under the Government Liability for Negligence Act[17] and are further covered by a Good

[13] "*Michigan Cyber Civilian Corps*," Michigan State Government Website.
[14] Interview with a volunteer coordinator from MiC3.
[15] "*Michigan Cyber Civilian Corps*," Michigan State Government Website.
[16] Interview with a project manager from MiC3.
[17] Governmental Liability Act, State of Michigan Act 170 of 1954, http://www.legislature.mi.gov/(S(fxm52p55rfo4giqitlzspcy5))/documents/mcl/pdf/mcl-act-170-of-1964.pdf.

Samaritan clause to facilitate their work on behalf of the state.[18] There are also protections for the state of Michigan. The state is not liable to a MiC3 volunteer for personal injury or property damage suffered through participation in the MiC3 activities.[19]

Operating Details

Command Chain for Deployment

Deployment of MiC3 originates with a cyber incident response request from a "client", which may be reported to the MSP, the law enforcement partner of the MiC3, or to the Michigan Cyber Command Center (MC3), who is responsible for cyber emergency response under the direction of the MSP.[20] The "client" of MiC3 refers to and includes municipalities, educational institutions, nonprofits, and/or business organizations that have requested rapid response assistance.[21] In response, the MC3 will discern whether the reported incident has a criminal nexus that needs investigation from the MSP or could be mitigated by the MC3 itself. Upon receipt of a cyber incident report, the MSP will investigate if necessary, and contact the MiC3 coordinator at the DTMB when appropriate. The volunteer coordinator would deploy the suitable members to respond to the cyber incident on behalf of the DTMB, based on availability, skill sets, and other factors.[22]

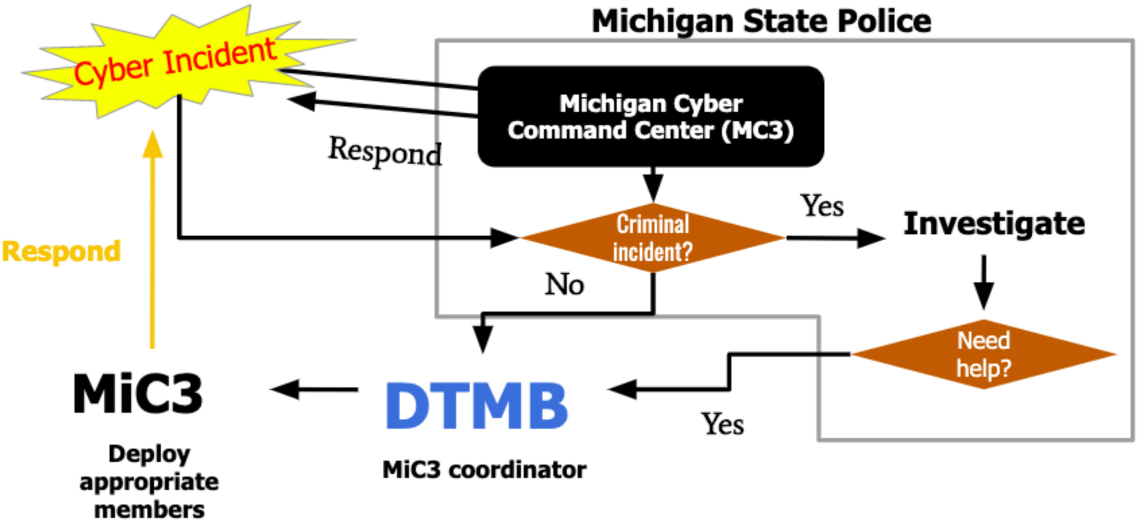


Figure 3. Cyber Incident Response Command Chain of the MiC3[23]

[18] "*Bridging State-level Cybersecurity Resources,*" Ruiz.
[19] State of Michigan Act 132 of 2017.
[20] Interview with a volunteer coordinator from MiC3.
[21] State of Michigan Act 132 of 2017.
[22] Interview with an executive of the Michigan State Police.
[23] Drawn by SIPA Capstone Project Team based on interviews with a volunteer coordinator of MiC3 and an executive of the Michigan State Police.

As previously mentioned, before the passage of state law (Act 132), the MiC3 had existed for three years. However, it had never deployed volunteers because deployment could only be activated if the governor declared a state of cyber emergency, which never occurred because the threshold for such an event was too high. With the passage of Act 132, a revised framework to guarantee the effectiveness of their operation was adopted, which lowered the threshold of deployment. This has led to MiC3's involvement in at least four incident responses during the past 2 years.[24]

Management

For effective management, a part-time MiC3 volunteer coordinator is employed by the DTMB with a contract functioning as the centralized leadership for this program. MiC3 members have monthly meetings that are primarily virtual live meetings. When they hold quarterly group meetings in person, they have participation from key partners such as MSP, the Federal Bureau of Investigation (FBI), the Central Intelligence Agency (CIA), the National Security Agency (NSA), and the National Guard.[25]

Challenges

2019 Audit Report

To assess the effectiveness of the DTMB's administration of the MiC3, the Michigan State Auditor General conducted the 2019 Performance Audit Report and concluded moderate effectiveness. The report alleged that the DTMB did not adequately contract with volunteers to ensure acceptance of the terms and conditions of membership in the program. And DTMB also failed to ensure that all volunteers underwent sufficient background checks; sufficiently evaluate the qualifications of all volunteers.[26]

The DTMB responded at a Michigan House Oversight Committee Meeting in October 2019 that they revised onboarding documents cleared by the Attorney General's Office to ensure compliance with Public Act 132. They designed and will soon commence implementation of an automated record-keeping system, which will reduce data entry and allow self-service capabilities for volunteers. Plans have been developed by the DTMB to improve the reporting capacity of assessing member location, expertise, and professional activities, and to increase governance.[27]

Appropriations

[24] Interview with a volunteer coordinator from MiC3.

[25] Interview with a project manager of MiC3.

[26] State of Michigan Office of the Auditor General, "*Performance Audit Report - Michigan Cyber Civilian Corps*," https://audgen.michigan.gov/wp-content/uploads/2019/09/r071051919-0007.pdf.

[27] Michigan Cyber Civilian Corps, "*House Oversight Committee Meeting*," October 10, 2019, https://mirsnews.com/pdfs/committeemeetings/10-10-2019%20-%20MI%20Cyber%20Security%20Corps%20-%20House%20Oversight.pdf.

The DTMB covers the vast majority of the MiC3's budget.[28]

Ohio Cyber Reserve (OhCR)

The Ohio Cyber Reserve (OhCR) is an initiative born from the partnership between the Adjutant General's Department and the Ohio Cyber Collaboration Committee (OC3), which is made up of more than 200 representatives from the public, private, military and educational organizations. Ohio State Governor Mike DeWine signed a Senate Bill on October 25, 2019, to develop a more robust cybersecurity infrastructure and workforce in the state.

Augmentation Needs & Mission Analysis

The state of Ohio recognized that cyber experts in Ohio, and especially in public sectors, are understaffed and as a result stretched thin. Small governmental entities and critical infrastructures need assistance in the assessment and best practices, as well as in responding to cyber events. There is also an education gap that needs to be addressed to meet the growing demand for cyber expertise. In response the Ohio Cyber Reserve (OhCR), has recommended that high school and college students be provided with more exposure to cybersecurity expertise and resources throughout their education.[29] This is in a key component to OhCR's mission, which can be categorized in the following three modules:

- **Assessment**

  The OhCR brings assessment support, advanced practices, and recommendations using NIST standards to the small-government organizations and critical infrastructures.

- **Education**

  OhCR members support education in colleges and universities in Ohio, including establishing cyber clubs and developing student mentorship programs, etc. Their goal here is to enlarge the future cybersecurity workforce by increasing the exposure during their school life.

- **Cyber Incident Response**

  OhCR members activate State Active Duty to assist in cyber incident response which is similar to the active duty when the National Guard activates out for other types of disasters and crises.[30]

Legal Framework

[28] State of Michigan Office of the Auditor General, "*Performance Audit Report - Michigan Cyber Civilian Corps*," https://audgen.michigan.gov/wp-content/uploads/2019/09/r071051919-0007.pdf.
[29] "*Ohio Cyber Reserve*," Ohio Cyber Collaboration Committee Website, accessed April 19, 2020, http://www.ohioc3.org/ohcr.
[30] Interview with a cybersecurity coordinator of the Ohio Adjutant General's Department.

The State-level legislation, Senate Bill 52, was signed into law by Governor Mike DeWine to create the OhCR.

What's more, Senate Bill 52 organizes the OhCR and a part of the Ohio organized militia under the Adjutant General's Department. The Adjutant General's Department develops appropriate policies to support and regulate the teams' behavior. While the OhCR is a component of the Ohio National Guard (ONG), it is explicitly not authorized for activation into Federalized military service for the United States.[31]

Membership

An OhCR member must be a U.S. national or a lawful permanent resident, and any person who has been expelled or dishonorably discharged from the armed forces will be disqualified from being accepted.[32] Team members are expected to have subject matter expertise with approximately five years of demonstrated focused effort in a cybersecurity discipline.[33]

The applicants have to go through an online application, self-assessment, SANS tests, and their submissions would be screened by the ONG's cyber team to determine the qualifications. After that, they are subject to an appropriate background check, under rules adopted by the Governor and Adjutant General, before admittance into the OhCR.[34]

To avoid legal issues, OhCR Members are expected to sign and adhere to non-disclosure agreements (NDA), a volunteer agreement, a code of conduct and ethics, a privacy act statement for OhCR administrative purposes, and an Acceptable Use Policy.[35]

Training and Exercises

Training is also emphasized very much in Ohio Cyber Reserve, where they receive individual training and additional training for each of the three missions, with Ohio Cyber Range functioning as a support platform for the professional training and communication.[36] To illustrate, Ohio Cyber Range is the tool of OC3 to support workforce development, cyber incident response team training, and a testbed for cyber

[31] Ohio Legislative Service Commission, "*Senate Bill 52 Final Analysis*," January 24, 2020, https://www.legislature.ohio.gov/download?key=12623.

[32] Ibid.

[33] Ohio Cyber Reserve Application Protocol, https://wss.apan.org/ng/ONG_CPT/OHCR/SitePages/Expectations.aspx.

[34] Interview with a cybersecurity coordinator of the Ohio Adjutant General's Department.

[35] Ohio Legislative Service Commission, "*Senate Bill 52 Final Analysis*."

[36] Interview with a cybersecurity coordinator of the Ohio Adjutant General's Department.

programs and systems. It also promotes learning and teaching for students and educators at the K-12 and collegiate levels.[37]

Legal Protection

Senate Bill 52 provides liability protection by specifying that OhCR members are not liable for any negligent acts performed within the scope of their duties.[38]

Operating Details

After individuals become members of the OhCR, they will be assigned two different statuses. The first one is their initial "volunteer status," which includes conducting their first and second mission. Deployment to a third mission is performed on a different status where the state pays the members. The pay rate is commensurate with state information technology employees who have comparable training, experience, and professional qualifications.[39]

The OhCR's plan for managing the deployment of volunteers is to organize them into ten regionally-based teams. Because Ohio is divided into five regions, this means there are two volunteer teams for each area. The original number of members in each team is ten, but they are hiring double to make sure there is availability when a cyber incident happens.[40] The teams will be provided training, equipment, and IDs and will work out of ONG armories. When deemed fully trained and certified, OhCR members will be available for call up to assist in the cyber response. As for the volunteers that are not adequately trained yet, but are vetted, they can be used to support student mentoring efforts under the OC3.[41]

Chain of Command

The Ohio State Governor, as the Commander-in-Chief of the OhCR, may order individuals or units of the Ohio Cyber Reserve to execute the State Active Duty directive to protect state, county, and local government entities and critical infrastructure. Upon request, the Governor also may order the OhCR to protect a business or citizen.

[37] "*Cyber Range*," Ohio Cyber Committee Website, accessed April 19, 2020, https://www.ohioc3.org/cyber-range.
[38] Ohio Legislative Service Commission, "*Senate Bill 52 Final Analysis*."
[39] Interview with a cybersecurity coordinator of the Ohio Adjutant General's Department.
[40] Ibid.
[41] Ohio Legislative Service Commission, "*Senate Bill 52 Final Analysis*."

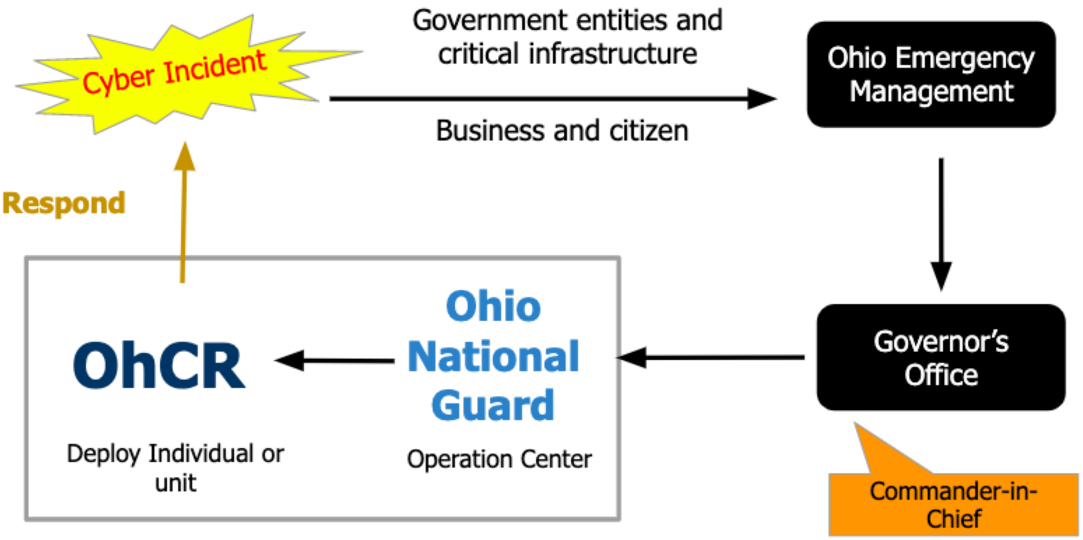


Figure 5. Cyber Incident Response Command Chain of the OhCR[42]

To receive assistance from the OhCR for incident response, the entities that need help must request assistance from the Governor's Office through the Ohio Emergency Management Agency. If the governor decides to direct the Ohio National Guard to respond, the Ohio National Guard's Operations Center will determine whether the guard's cyber unit should respond or if it is a more appropriate task for the OhCR.[43]

Management

OhCR employs a dedicated full-time cybersecurity coordinator in the Adjutant General's Department to coordinate with several different state agencies, as well as colleges, universities, local governments, who have an interest in cybersecurity. This position also is the coordinator of the OhCR with all other stakeholder entities.

Appropriations

The Adjutant General received appropriations with $100,000 for FY 2020 and $550,000 for FY 2020 for creating and maintaining OhCR.[44]

Estonian Defence League Cyber Defence Unit (EDL CDU)

The Estonian Defence League Cyber Defence Unit (EDL CDU) is regarded as the federal-level volunteer corps in the cybersecurity arena for government support. Being a volunteer organization and a civil-military agency aimed at protecting Estonian

[42] Drawn by SIPA Capstone Project Team based on an interview with a cybersecurity coordinator of the Ohio Adjutant General's Department.
[43] Interview with a cybersecurity coordinator of the Ohio Adjutant General's Department.
[44] Ohio Legislative Service Commission, "*Senate Bill 52 Final Analysis*."

cyberspace, the EDL CDU was established on the grounds of the 2007 attack on the country's leading information infrastructure that paralyzed critical services, in a country that highly relies on digital services.

Augmentation Needs & Mission Analysis

The EDL CDU's mission is to protect Estonia's highly digitalized society, including the protection of information infrastructure and supporting two broad types of objectives: capability building and operations.

The aim of the CDU's capability building includes developing a reserve of experts and a network of cooperation, including crisis response. Another point is to promote awareness, education, and training both by providing continuous information security education and training to members. The objective of operations refers to improving the security of civil critical information infrastructure by raising their security level, organizing cyber defense exercises, regularly disseminating best practices, and enhancing preparedness for operating during a crisis.[45]

Legal Framework & Authorities

The principles and guidelines for membership and operation of the EDL CDU are established by federal Estonian law, "The Estonian Defense League Act" (referred to as "the Act") approved by the Government of the Republic in 2013.

As defined in the legislation, the Estonian Defence League (EDL) is a voluntary national defense organization operating within the competency of the Ministry of Defence (MoD). It serves as an extended response capability and is allowed to be called upon when additional help is needed.[46]

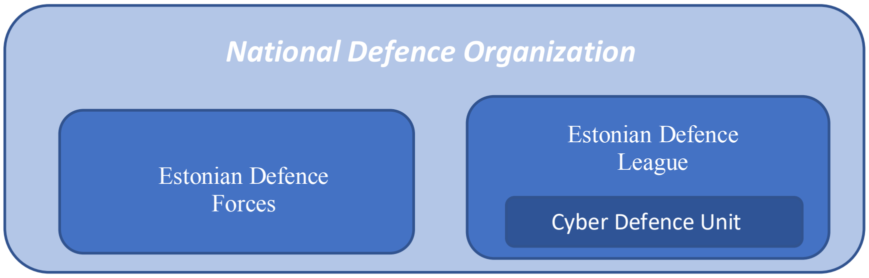


Figure 6. Organizational Framework of the EDL CDU[47]

The Act explicitly integrates the CDU into the national defense system, providing it with a legally established objective. As one of the structural units of the EDL, the CDU

[45] "*The Estonian Defence League's Cyber Unit*," Estonian Defence League Website, accessed April 19, 2020, https://www.kaitseliit.ee/en/cyber-unit.

[46] The Estonian Defence League Act, April 1, 2013, https://www.riigiteataja.ee/en/eli/510032015001.

[47] Drawn by SIPA Capstone Project Team based on the Estonian Defence League Act, Ibid.

operates under the same legal framework and is led by a unit commander who directly reports to the commander of the EDL.[48]

Membership

Admittance Requirements & Steps

Any individuals interested in joining the CDU have to be an active member of the EDL to be qualified for application.[49] What is different from Michigan and Ohio is that applicants for the EDL CDU are not rigorously required to have cybersecurity expertise and could be supplemented by other relevant skills related, including legal, policy, educational, and project management expertise. Nevertheless, to join the CDU, the applicant must go through a screening procedure and obtain a security clearance.[50] Further to obtain membership, a written request that is directed to the commander of the CDU is needed, and a recommendation by an existing CDU member is preferred. Applicants have to pass background checks and can perform an oath of loyalty before officially admitted.[51]

Liability & Disciplinary Action

Members of the CDU are personally and financially responsible for the means granted to them by the EDL. For disciplinary offenses committed, members of the CDU are liable to disciplinary action under the framework applicable to all members of the EDL. Disciplinary authority lies with the commander of the CDU, and disciplinary offenses include damage to the image of the EDL, non-compliance with the legal requirements for members' duties, as well as non-compliance with an order.[52]Liability would not occur if they are performing within the scope of their duty and the activities are not causing any damage to the interest of the EDL.

Operating Details

Conditions & Procedures for EDL CDU Deployment

The Emergency Act permits recourse to the EDL, including the CDU, if a public authority is unable to resolve the emergency or do so on time.[53] During emergencies caused by cyber events, the primary body to determine the necessity of involving the

[48] Monica M. Ruiz, "Is Estonia's Approach to Cyber Defense Feasible in the United States?" January 9, 2018, https://warontherocks.com/2018/01/estonias-approach-cyber-defense-feasible-united-states/

[49] Kadri Kasha, "*The Cyber Defense Unit of the Estonia Defense League – Legal, Policy and Organizational Analysis*," 2013, https://ccdcoe.org/uploads/2018/10/CDU_Analysis.pdf.

[50] Interview with a former senior executive engaged in the organizing process of EDL CDU.

[51] Kasha, "*The Cyber Defense Unit of the Estonia Defense League – Legal, Policy and Organizational Analysis*."

[52] The Estonian Defence League Act.

[53] Emergency Act, August 2, 2017, https://www.riigiteataja.ee/en/eli/ee/513062017001/consolide.

CDU would be the State Information System's Authority, whose function includes the management of state information system security and supervision over the security of nationally critical information systems. Other bodies to potentially involve the CDU include the Ministry of Interior, Police and Border Guard Board, the Rescue Board, and the Internal Security Service, as well as other offices bearing internal security tasks.

The request to involve the CDU is to be addressed to the Commander of the EDL, which has to include the purpose of engaging the CDU, together with an outline of the projected tasking. The discretion of the Commander of the EDL has to involve the urgency of the potential threat to critical infrastructure and the possible danger to the health and lives of people as well as to property and environment. The availability of suitably skilled members, the effect of the Unit's engagement on the other tasks of the EDL, and the foreseeable costs involved are also to be considered.[54]

Appropriations

Estonian state funds cover the vast majority of the unit's budget.[55]

Challenges

Efficiency and the Synchronization of Efforts

Ensuring the time volunteers contribute to the unit's efforts is used efficiently and the harmonization of different availabilities and skill sets within the group can be difficult. Though the EDL CDU has enough volunteers to respond, it is a challenge to guarantee the availability of individuals with specific knowledge and skills when incidents require them. To address that, the leadership of CDU must keep clear records of personal member's skill sets and status, often communicating and maintaining relationships with its members directly.[56]

Coordinating with Private Cybersecurity Firms

Despite the benefits of EDL CDU to the security of the whole society in Estonia, there still could exist conflicts of interest for both employees of cybersecurity firms who may want to volunteer and between the CDU and the firm. The key to avoiding them is communication and writing agreement. Ultimately, it is the individual's choice to join, hence proper communication of what is expected should be addressed with their employers beforehand.[57]

[54] Kasha, "*The Cyber Defense Unit of the Estonia Defense League – Legal, Policy and Organizational Analysis*."

[55] Interview with a former senior executive engaged in the organizing process of EDL CDU.

[56] Monica M. Ruiz, "*Establishing Volunteer US Cyber Defense Units: A Holistic Approach*," December 7, 2017, https://ieeexplore.ieee.org/document/8167512.

[57] Interview with a former senior executive engaged in the organizing process of EDL CDU.

Key Takeaways from Cybersecurity Case Studies

To conclude our analysis of the above cybersecurity case studies, we offer the following notable takeaways that we believe are most relevant for NYC3's volunteer corps framework:

- **Legislation**: Codified legislation at the state level is the choice for most of the cyber cases we have studied. NYC3 will want to consider appropriate comparable legal protections to grow with the maturity of the volunteer program as needed beyond its existing executive order.
- **Lifecycle**: Incident Response is not the only point on the lifecycle that NYC3 could leverage the deployment of volunteers to step on. Assessment and educational support could also be good fields for a volunteer corps to contribute to NYC3's overall mission.
- **Volunteer Agreements**: To address some legal concerns, and maintain a relationship of the corps with other entities, mechanisms to protect the official identity of volunteers with NYC3 should be considered. Non-disclosure Agreement (NDA) is a common requirement for members by a cyber volunteer corp.
- **Training**: Both the MiC3 and the OhCR emphasize post-admission training for corps members. Some high-quality training is deemed too expensive for employers thus for volunteers, training could serve as an incentive as well as a platform to network.
- **Experience**: For recruiting volunteers, certain technical certificates might not be the sole measurement. From our interviews and research, we learned it is worth considering demonstrated experience and practical skills in the selection process of appropriate volunteers.
- **Volunteer Engagement:** The MiC3 aimed at and succeeded in building a volunteer community where they communicate and improve, through meetings and training opportunities to keep them active and motivated. The OhCR is also doing so by allowing volunteers to perform more frequently in assessment phases of the CLC and in education missions.

Non-Cybersecurity Volunteer Models

Volunteers have played active and vital roles in a variety of non-cybersecurity events and projects, motivated by individual desire to serve local, industry, and community needs. The forms of non-cybersecurity volunteer projects are highly diversified. Non-professional volunteers in disaster relief, for example, are not necessarily formally registered and they can contribute in various ways, including manual labor or information sharing on social media. Whereas, professional volunteers—as explored in cybersecurity cases—are often registered experts who may be activated to respond to community needs by taking advantage of their expertise.

This section examines four prominent cases of volunteer engagement in non-cybersecurity projects, from emergency response to international capacity building in the financial sector, and extracts lessons learned focusing on (1) operationalization of volunteers; (2) recruitment and retention of volunteers for highly demanding roles; (3) benefits of industry engagement; and (4) effective use of professional expertise through volunteer projects in each of the case studies. The lessons from different aspects and contexts of these volunteer engagement efforts will provide clues on what elements are required when designing NYC3's volunteer framework.

Operationalization: Hurricane Sandy

Over a month after Hurricane Sandy hit NYC in October 2012, it is estimated that more than 11,000 volunteers worked tirelessly to help New Yorkers and the City recover from the storm.[58] The volunteers including the City's Community Emergency Response Team (CERT), corporate groups, individuals, and community organizations knocked on doors, mucked out homes, cleaned up parks, and staffed grassroots neighborhood distribution centers by ad hoc or organized participation, taking advantage of their skills, resources, and enthusiasm. Over 1,200 medical volunteers from the City's Medical Reserve Corps are the primary example of professionals who worked throughout the storm.[59] The City opened eight Special Medical Needs Shelters, where these volunteers worked with medical professionals and administration from the Health and Hospitals Corporation, mental health professionals from the Department of Health and Mental Hygiene, and federal Disaster Medical Assistance Teams (DMATs).

[58] Linda I. Gibbs and Caswell F. Holloway, "*Hurricane Sandy After Action: Report and Recommendations to Mayor Michael R. Bloomberg*," May 1, 2013, https://www1.nyc.gov/assets/housingrecovery/downloads/pdf/2017/sandy_aar_5-2-13.pdf, 29.
[59] Ibid., 16-17.

Photo 1. Volunteers cleaned up parks, beaches, and recreation centers, collected debris, and distributed millions of meals (Photo by Luna Park Coney Island[60])

Operational Lessons

Through response and recovery activities during and after Sandy, both government coordinators and on-the-ground responders, including volunteers, identified communication and coordination among a variety of stakeholders, either across and within organizations, as a critical operational challenge.

Government agencies at the time were, in particular, confronted with difficulties in effectively deploying teams of people and goods. CERT volunteers, who were activated by the local sponsoring government agencies in the neighboring states of New York, recognized that keeping the team organized during the storm and ensuring deployed volunteers had the support they needed were the most difficult tasks—research by the Federal Emergency Management Agency (FEMA) in September 2014 shows.[61] At the U.S. Senate hearing in March 2013 titled "Rebuilding After Hurricane Sandy," Brad Gair, Director of Housing Recovery Operations for NYC, stressed the vital role of the government in tackling the issue in communication and coordination.[62] According to an after-action report commissioned by Mayor Mike Bloomberg and released in May 2013, the City sees that they needed more thorough pre-planning concerning volunteers on communications and protocol plan, policy and procedures of

[60] https://www.flickr.com/photos/59466009@N02/8179611271.

[61] U.S. Federal Emergency Management Agency, "*Lessons Learned by CERT Volunteers During Sandy Activation*," September 8, 2014, https://www.fema.gov/media-library-data/1410972738212-81f62d206e57b3a3a1e83ecd0de11e24/20140908_Lessons_Learned_by_CERT_Volunteers_During_Sandy_Activation_Final_Draft_v4.pdf, 2.

[62] U.S. Government Publishing Office, "*Rebuilding After Hurricane Sandy: Hearing Before A Subcommittee of the Committee on Appropriations United States Senate One Hundred Thirteenth Congress*," 2015, https://www.govinfo.gov/content/pkg/CHRG-113shrg80071/pdf/CHRG-113shrg80071.pdf, 42.

information sharing, and screening process to let volunteers work in sensitive environments.[63]

With the hodge-podge of official and unofficial groups and the steady stream of ad hoc individuals, volunteers on the ground also experienced challenges in communicating or making operational coordination with other groups or government agencies like the Office of Emergency Management (OEM). According to Jacob Siegel, a non-professional volunteer who worked as part of a volunteer organization in the Sandy response, volunteers had to drive around with supplies until they found people who needed them realizing the lack of operational information on the ground.[64] Siegel sees, in this case, the function of gathering intelligence and feeding it into a single model was not working effectively at the command-and-control level. From the viewpoint of medical professionals and professional volunteers who responded to Sandy in hospitals and Emergency Medical Services (EMS) groups, organizational barriers, such as a lack of responders' representation in the government's emergency planning process or immature working relationships between career and volunteer professionals, were identified as a key contributing factor of operational challenges.[65] A high-ranking official in a prominent volunteer organization who worked closely with the City government also suggests this point explicitly in the NYC context, concerning the relationship among the OEM, the Mayor's Office, the New York Police Department (NYPD), and non-government entities such as Voluntary Organizations Active in Disaster (VOAD) that bring together volunteer groups to plan and coordinate relief efforts.[66]

The lessons learned from these post-action analyses from different perspectives are, in fact consistent, and can be summarized as follows:[67, 68]

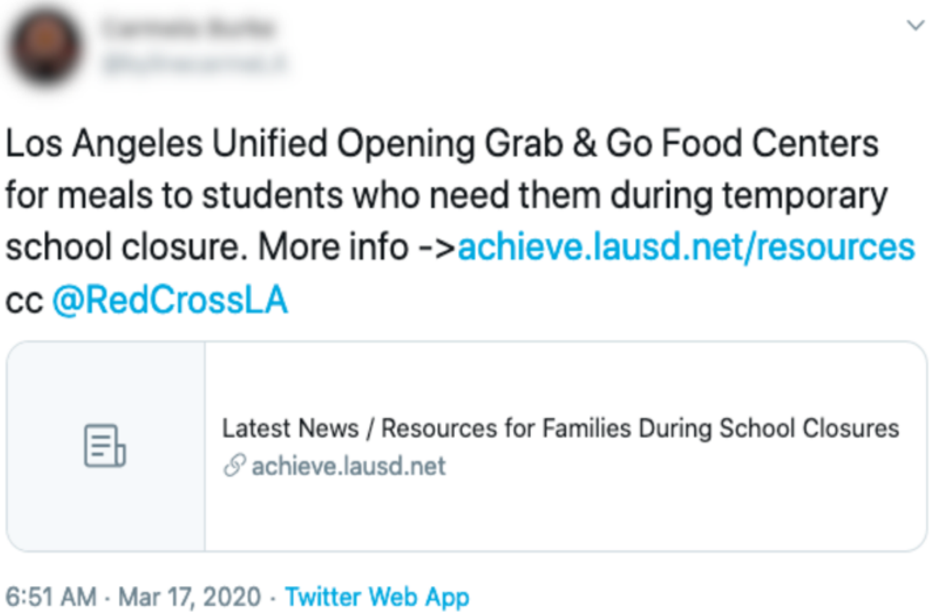
- Develop a transparent, specific chain of representation for emergency planning and operations with the inclusion of response stakeholders.
- Have the area of volunteer's responsibility clearly defined, and give instructions to volunteers so that they can work within the command-and-control structure.
- Do as much advance work as possible before deployment of volunteers.

[63] Gibbs and Holloway, "*Hurricane Sandy After Action: Report and Recommendations to Mayor Michael R. Bloomberg*," 30.
[64] "*A Gap in the City's Hurricane Response, and a Volunteer Army's Attempt to Fill It*," Jacob Siegel, December 18, 2012, https://www.politico.com/states/new-york/albany/story/2012/12/a-gap-in-the-citys-hurricane-response-and-a-volunteer-armys-attempt-to-fill-it-067223.
[65] American College of Emergency Physicians, "*Lessons Learned from Hurricane Sandy and Recommendations for Improved Healthcare and Public Health Response and Recovery for Future Catastrophic Events*," December 22, 2015, https://www.acep.org/globalassets/uploads/uploaded-files/acep/by-medical-focus/disaster/lessons-learned-from-hurricane-sandy-webpage.pdf, 17-19.
[66] "A Gap in the City's Hurricane Response, and a Volunteer Army's Attempt to Fill It," Siegel.
[67] Gibbs and Holloway, "*Hurricane Sandy After Action: Report and Recommendations to Mayor Michael R. Bloomberg*," 30.
[68] U.S. Federal Emergency Management Agency, "*Lessons Learned by CERT Volunteers During Sandy Activation*," 2-3.

Digital Volunteers

In the Hurricane Sandy response, nonprofit and volunteer organizations stepped in to assist in developing and combining information resources and making them available for the public and response stakeholders.[69] Among them, the Red Cross Digital Volunteers set a good model of volunteer engagement (non-professional) designed to provide informational support in emergency response.

The American Red Cross Digital Volunteers are tasked to assist the National Social Engagement team of American Red Cross's National Headquarters which responds to thousands of daily social mentions of the Red Cross to curate them into its social media update.[70] During disaster and non-disaster times, digital volunteers monitor online conversations for disaster-affected people who may need help, share disaster updates and resources through personal social media accounts, and offer a compassionate voice to people who have been impacted.[71]



Los Angeles Unified Opening Grab & Go Food Centers for meals to students who need them during temporary school closure. More info ->achieve.lausd.net/resources cc @RedCrossLA

Latest News / Resources for Families During School Closures
achieve.lausd.net

6:51 AM · Mar 17, 2020 · Twitter Web App

Photo 2. Red Cross Digital Volunteers help those in need by providing them with key information (Example: screenshot from Twitter)

During the Sandy response, digital volunteers tracked more than 2 million online posts for review, choosing specific keyword searches relevant to Red Cross services,

[69] U.S. Department of Homeland Security, "*Lessons Learned: Social Media and Hurricane Sandy*," June 1, 2013, https://www.dhs.gov/sites/default/files/publications/Lessons%20Learned%20Social%20Media%20and%20Hurricane%20Sandy.pdf, 8.

[70] American Red Cross, "*Social Engagement Handbook Version 2.0*," June 2012, http://redcrosschat.org/wp-content/uploads/2012/06/SocialEngagementHandbookv2.pdf, 5.

[71] "*How to Become a Digital Volunteer*," American Red Cross, accessed April 9, 2020, https://redcrosschat.org/digitalvolunteer/.

such as shelter and emotional support, where 229 posts were sent to the National Headquarters, and 88 resulted in a change in action on ground operations.[72] Digital volunteers have also assisted Red Cross's service delivery efforts and those affected in other subsequent hurricanes, such as Hurricane Matthew in 2016, where these volunteers served as part of the newly-launched Red Cross Dallas Digital Operations Center to share emergency preparedness information.[73]

Digital volunteers sign up to monitor, engage, and report in four-hour shifts, and the work is done remotely in coordination with their local chapter communicators.[74] One can be a digital volunteer just by registering online, contacting local Red Cross Volunteer Services, and taking the Social Basics course online on the skill sets in need in the region. The applicants must meet requirements of time commitment and familiarity with technical tools involved in this role, such as social media monitoring tools.

Recruitment & Retention: Firefighters and EMS

Volunteer fire and emergency medical services are a long-standing tradition in the U.S. that often encompass families, generation after generation. According to a report by the U.S. Fire Administration (USFA) released in May 2007,[75] however, fire departments today are experiencing more difficulties with recruiting and retaining volunteers for these highly-demanding roles than ever before.

[72] U.S. Department of Homeland Security, "*Lessons Learned: Social Media and Hurricane Sandy*," 20.

[73] "*Dallas Red Cross Launches Digital Operations Center in Response to Hurricane Matthew*," American Red Cross North Texas Region, October 7, 2016, https://redcrossntxblog.com/2016/10/07/dallas-red-cross-launches-digital-operations-center-in-response-to-hurricane-matthew/.

[74] "*How to Become a Digital Volunteer*," American Red Cross.

[75] U.S. Fire Administration, "*Retention and Recruitment for the Volunteer Emergency Services: Challenges and Solutions*," May 2007, https://www.usfa.fema.gov/downloads/pdf/publications/fa-310.pdf.

Photo 3. Volunteer firefighter of New York State are organized at the county and regional level, including those in the five NYC boroughs[76] (Photo by storm2k[77])

Through a field survey, the USFA sees that there is no single reason for the decline in volunteers. Still, the problems can often be traced to several underlying factors such as more demands on people's time in a hectic modern society, more stringent training requirements,[78] internal leadership problems and a decline in the sense of civic responsibility.[79] The following are lessons learned from USFA's case studies:[80]

- Administrators at the top should know the personnel, their needs, and how to manage the human aspects of volunteering, or there will be recruitment and retention problems.
- Volunteer organizers should consider financial incentives, duty shifts, and how training is delivered, among others, to make volunteering more palatable.
- Volunteer programs should recognize that volunteers, many of whom are "hands-on" type people like to do something that leads to a purpose.
- Whatever transpires within the department must be ethical, impartial, and fair to all.

The USFA research also identifies key contributing factors of volunteer retention and recruitment problems.[81] Their findings include vital elements that provide

[76] Southern New York Volunteer Firemen Association Website, accessed on April 9, 2020, http://snyvfa.org/.
[77] https://www.flickr.com/photos/67083659@N00/460244640.
[78] See Ibid., 8 for national standard training modules for firefighters and EMS personnel, the average length of the courses, and approximate time to complete them for volunteers.
[79] Ibid., 2.
[80] Ibid., 170.
[81] See Ibid., 7 for the comprehensive list of the sources of problems and the contributing factors.

particularly useful implications for the NYC3's cyber volunteer framework, such as[82] participatory management; clear mission statement; training of the Chief and officers; excellent internal communication; assignment of a volunteer coordinator; visibility and image of volunteer departments; collaboration with local politicians; liability coverage; alleviating the burdens of paperwork for volunteer responders; realistic training; management of time demands; recognition for volunteers; incentive programs; coordinated, systematic recruitment and screening; and clarification of volunteer responsibility (see Appendix 1 for a further description for each element).

As a legislative foundation for volunteer recruitment and retention, the State of New York has the following laws[83] providing benefits for volunteer fire and emergency medical services who work in the same line of duty with full-time career responders:[84]

- General Municipal Law that authorizes the establishment of defined benefit service award programs to provide municipally funded, pension-like benefits.
- Volunteer Firefighters' Benefits Law, Workers' Compensation Law, and Retirement & Social Security Law that provide for cash benefits and medical care to volunteer firefighters and EMS workers who are injured or become ill in the line of duty.
- Tax Law that provides for a real property tax exemption for volunteer firefighters and EMS workers.

In addition to the State legislation, the Firemen's Association of the State of New York (FASNY), a nonprofit organization dedicated to informing, educating, and training New York volunteer firefighters, independently offer a variety of benefits, services, and discounts for its members such as The Accidental Death and Dismemberment program; training and education programs; membership of the FASNY Federal Credit Union; scholarships; and service recognition awards.

Industry Engagement: New York State COVID-19 SWAT Team

On March 24, 2020, New York State launched the first-in-the-nation technology service partnership, dubbed COVID-19 Technology SWAT team, calling for technology professionals to assist with an unprecedented need for new software and application development across State agencies posed by the massive response to the COVID-19 pandemic.[85] By partnering with global technology companies, the State's Office of Information Technology Services (ITS) and the Department of Financial Services, the

[82] Ibid., 29, 32, 38, 44-45, 48, 54, 60, 79, 81, 88, 93, 95, 100, 132, and 151-153.
[83] "*New York Survivor Benefits*," National Fallen Firefighters Foundation, last updated in November 2018, https:// www.firehero.org/resources/family-resources/benefits/local/ny/.
[84] New York State Department of Health, "*Learn About your Local Fire Service*," last updated in December 2010, https://www.health.ny.gov/prevention/injury_prevention/children/toolkits/fire/docs/learn_about_local_fire_services.pdf, 1.
[85] "*New York Launches IT 'SWAT Teams' to Aid Pandemic Response*," Benjamin Freed, March 25, 2020, https://statescoop.com/new-york-it-swat-teams-aid-pandemic-response/.

organizers of the state effort, aim to augment their workforce capacity to complete projects more quickly. They also hope to harness a proven spirit of goodwill of New Yorkers in a time of crisis.

The program had relatively quick uptake. The State teamed up with Microsoft, Google, and Apple, as well as Tech:NYC, a trade organization representing NYC's tech industry.[86] Microsoft's self-screening and scheduling tool, which allows individuals to assess risk factors associated with COVID-19 and connects them to the State's COVID testing resources, has already been used by more than 100,000 New Yorkers within three weeks after the launch of the initiative.[87] While the priorities of the State may change rapidly in response to the conditions on the ground, the team is expected to address further the digital infrastructure expansions needed for facilitating coronavirus testing; improving remote access to social services impacted by the pandemic like unemployment claims; digital delivery of public-health guidance; and IT support for the emergency centers and field hospitals that are being erected.[88]

In this initiative, the State seeks people and organizations that have professional experience in product management, software development and engineering, hardware deployment and end-user support, data science, operations management, design, and other similar areas.[89] Priority is being offered to teams of individuals who come from the same institution with minimum 90-day deployment periods, because the State is looking to maximize effectiveness by sourcing talent that already works together, thereby bypassing the process to figure out how to work together. The projects include options for participating either with on-site staffing or remotely.[90] When working as part of the team, tech professionals are allowed to access specific data necessary for a project, in tight compliance with all applicable federal and state laws, regulations, policies, and standards, under the State's control.

Effective Use of Highly Specialized Experts: Financial Services

Financial Services Volunteer Corps (FSVC) is a not-for-profit organization founded in 1990 in the U.S.[91] to advance economic development by strengthening financial

[86] Ibid.
[87] "*New York State's Self-Screening and Scheduling Tool Helping to Fight COVID-19*," New York State, April 15, 2020, https://www.ny.gov/updates-new-york-state-covid-19-technology-swat-teams/new-york-states-self-screening-and-scheduling.
[88] "*New York Launches IT 'SWAT Teams' to Aid Pandemic Response*," Freed.
[89] "*New York State Seeks Tech Talent for Its COVID-19 Technology SWAT Team*," Darrell Etherington, March 25, 2020, https://techcrunch.com/2020/03/25/new-york-state-seeks-tech-talent-for-its-covid-19-technology-swat-team/.
[90] Ibid.
[91] Kathie Beans, "*Banker Volunteers Help Bring Financial Stability to Emerging-Market Countries*," the RMA Journal, January 2013, https://reynoldswilliams.com/wp-content/uploads/2013/01/Merrill-Reynolds-International-Training.pdf, 45.

sectors in developing countries.[92]

FSVC delivers practical technical assistance internationally to public and private sector institutions in host countries, in areas such as strengthening central banking capacity. Volunteers are senior-level financial sector professionals who serve as unpaid experts. FSVC's model shows the key advantage of engaging professionals as volunteers: they can provide not only their expertise and experience of leading practices but also inherently objective training and advice. A significant number of FSVC volunteers are from U.S. regulatory authorities and the big U.S. banks.[93] They are required to meet the qualifications of commitment to objectivity and social responsibility, in addition to a minimum of 10 years of experience as finance, legal, and business professionals.[94] The volunteers work in strict confidence with local partners since institutions often do not want to advertise their problems or that they relied on a U.S.-based not-for-profit to find a solution to those problems.

FSVC's programs are demand-driven, where local partners request targeted technical assistance to address self-identified challenges,[95] and efficient matching of project needs and expertise is the critical component of their volunteer deployment. FSVC uses a central database so that the best volunteers can be identified out of several thousands of registered professionals when project requests in their area of specialization come.[96] For this purpose, experts are asked to answer a questionnaire that helps FSVC figure out their areas of knowledge and thus plug their profiles into the database.[97] While FSVC does not provide specific incentive programs other than payment for all travel expenses, professionals can gain knowledge of local financial markets and economies, lasting relationships with a global network of professional contacts, and other advantages for their career through experience as volunteers.[98] The safety of volunteers is often a problem as they pursue the mission,[99] and thus, FSVC works closely with the U.S. State Department to protect their volunteers abroad.[100]

Key Takeaways from Non-Cybersecurity Case Studies

To conclude our analysis of the above non-cybersecurity case studies, we offer the following notable takeaways that we believe are most relevant for NYC3's volunteer corps framework:

[92] "*Who We Are*," Financial Services Volunteer Corps, accessed April 9, 2020, https://www.fsvc.org/who-we-are/.

[93] Beans, "*Banker Volunteers Help Bring Financial Stability to Emerging-Market Countries*," 47.

[94] "*Benefits & Requirements*," Financial Services Volunteer Corps, accessed April 9, 2020, https://www.fsvc.org/volunteer/benefits-and-requirements/.

[95] "*Who We Are*," Financial Services Volunteer Corps.

[96] Beans, "*Banker Volunteers Help Bring Financial Stability to Emerging-Market Countries*," 47.

[97] Ibid.

[98] "*Benefits & Requirements*," Financial Services Volunteer Corps.

[99] Interview with one of the current organizers in the Financial Services Volunteer Corps.

[100] Beans, "*Banker Volunteers Help Bring Financial Stability to Emerging-Market Countries*," 46.

- **Preparedness:** Deployment of volunteers in emergency response requires government organizers to do thorough and inclusive advance work, with a comprehensive and transparent representation of stakeholders for planning processes and providing framework and opportunities to alleviate organizational barriers.
- **Program Design**: Though key factors and best practices for recruitment and retention of volunteers for highly-demanding roles have been identified through past examples, there is no one single volunteer framework that works in all cases. Administrators and volunteer organizers should properly assess and understand the personnel and their needs, to design more palatable volunteer programs.
- **Effective Use of Experts:** When engaged as volunteers, highly specialized professionals can not only share their expertise in leading practices, but also provide objectivity. This advantage can be ensured by requiring applicants to meet the qualification of commitment to objectivity, in addition to expertise requirements. Structured matching of professional volunteers and project needs can also facilitate effective use of volunteer expertise on the framework.
- **Public-Private Partnership:** Industry engagement provides efficiency by taking advantage of existing working relationships of professionals within organizations and of the influence that the private sector partners already have.
- **Potential Volunteer Roles:** Supportive volunteer functions in non-cybersecurity projects, such as advisory and informational support during emergency response, can also be possible role models for NYC3’s cyber volunteer corps.

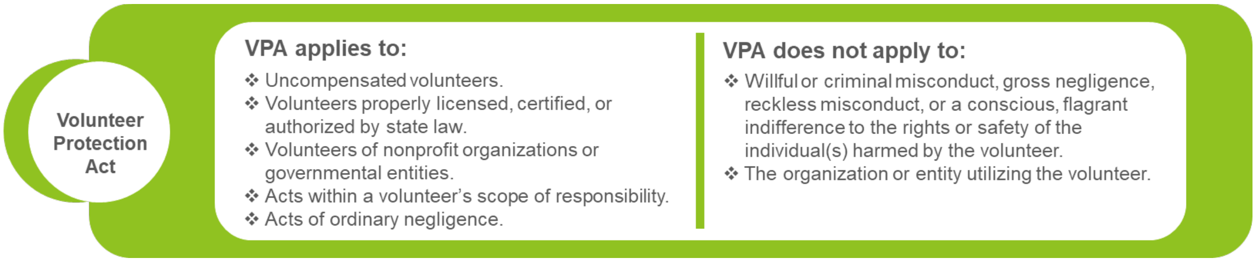
LEGAL CONSIDERATIONS

Legal considerations for the protection of the organization and its volunteers were pervasive in our research. It is further noteworthy that we have not conducted an in-depth legal analysis of federal, state, and local laws. Nevertheless, based on the case study takeaways, as well as insights from interviews, we have come up with several key legal considerations that could be important for the greater use and deployment of a volunteer program for NYC3 as related to cyber response:

Immunity Coverage for Volunteers and NYC3

Volunteers themselves and the entities that recruit, deploy, and manage volunteers can be subject to liability in specific instances. As such, protection from liability often depends on the nature of the services provided and the emergency response program through which the volunteer is deployed. Depending on the roles across the cybersecurity life cycle (e.g. educating, advising, hands-on keyboard) that NYC3 assigns to volunteers, the appropriate legal protections should follow. This is to mean that NYC3 should ensure that any legal impediments to volunteering are addressed such as uncertainty about whether a volunteer and the entity that recruits and manages volunteers could be held liable is a significant deterrent to volunteering.

Volunteer protection clauses, or similar provisions, can be found at the federal (Federal Volunteer Protection Act: VPA[101]) and state levels (Good Samaritan Laws). The federal VPA does not protect entities that use the volunteers. Good Samaritan laws, on the other hand, allow states to pass legislation with greater protections for volunteers. As with other volunteer protection statutes, however Good Samaritan laws do not cover gross negligence.



VPA applies to:

- Uncompensated volunteers.
- Volunteers properly licensed, certified, or authorized by state law.
- Volunteers of nonprofit organizations or governmental entities.
- Acts within a volunteer's scope of responsibility.
- Acts of ordinary negligence.

VPA does not apply to:

- Willful or criminal misconduct, gross negligence, reckless misconduct, or a conscious, flagrant indifference to the rights or safety of the individual(s) harmed by the volunteer.
- The organization or entity utilizing the volunteer.

Figure 6. Volunteer Protection Act[102]

[101] U.S. Volunteer Protection Act of 1997, Pub. L. No. 105-19. Codified at 42 U.S.C. §§ 14501, http://www.gpo.gov/fdsys/pkg/PLAW-105publ19/pdf/PLAW-105publ19.pdf.

[102] "*Volunteer Protection Acts and Good Samaritan Laws,*" ASTHO Legal Preparedness Series, https://astho.org/Programs/Preparedness/Public-Health-Emergency-Law/Emergency-Volunteer-Toolkit/Volunteer-Protection-Acts-and-Good-Samaritan-Laws-Fact-Sheet/.

In New York State, Good Samaritan clauses only cover volunteer immunity for emergency medical treatment,[103] volunteer firefighters,[104] first aid responders in ski areas,[105] and for calling for 911 in drug/alcohol overdose situations.[106]

To provide immunity coverage for volunteers, an optimal solution would be a separate codified act that will create liability immunity for both volunteers themselves and their deploying organizations. For example, an analogous good practice can be seen in Michigan, which passed the Michigan State Cyber Civilian Corps Act[107] to shield volunteers from liability concerns as related to their work for MiC3.

Protecting Sensitive Information During Volunteer Deployment

Other concerns about the deployment of cyber volunteers has to do with the protection of sensitive private information. One answer to this problem could be a City law that establishes appropriate procedures for volunteers that are designed to protect any unauthorized disclosure of confidential information acquired by the participating volunteers. Such mechanisms could include:

- Signing confidential disclosure agreements;
- Detailed background screening;
- Attestation that volunteers meet NYC3's expectation of professional expertise;
- Requiring volunteers to avoid conflicts of interest that might arise from a particular deployment.

Private Sector Considerations

The experience of MiC3 showed that one of the challenges for enacting a state-run volunteer program was that the program could be deemed anti-competitive:[108] there was a concern that local cyber companies would be shut out of business opportunities, hindering the private sector.

To address this concern, a City law could be passed that creates clear volunteer deployment conditions. For example, it could be clarified that: (1) the program is meant

[103] §3000-A: Emergency Medical Treatment, New York State Public Health Law (Current through 2020 released Chapters 1-25), https://www.nysenate.gov/legislation/laws/PBH/3000-A.

[104] Good Samaritan Volunteer Firefighters' Assistance Act, 2003 N.Y. ALS 41; 2003 N.Y. LAWS 41; 2003 N.Y. A.N. 1401 (April 15, 2003).

[105] §1: Immunity from Liability, NY CLS Unconsol Ch. 211-A (Current through 2020 released Chapters 1-25) https://advance-lexis-com.ezproxy.cul.columbia.edu/api/document?collection=statutes-legislation&id=urn:contentItem:5CT3-2F71-6RDJ-84XM-00000-00&context=1516831

[106] New York State's 911 Good Samaritan Law. https://www.health.ny.gov/publications/0139.pdf.

[107] State of Michigan Act 132 of 2017.

[108] State of Michigan House Fiscal Agency, "*Legislative Analysis: Cyber Civilian Corps Act*," November 13, 2017, https://www.legislature.mi.gov/documents/2017-2018/billanalysis/House/pdf/2017-HLA-4508-C5F4E5CB.pdf, 5.

to aid only with large-scale or disaster-type cyber incidents and not designed to deploy volunteers to everyday incident responses, and/or that (2) cyber volunteers will take roles across the cybersecurity life cycle, where the private sector may not have particular interest to be involved, such as community education; thus, leaving for the private sector a wide array of events to respond to.

Mutual Aid Agreements with Other Cyber Corps

A myriad of policies aimed at improving cyber preparedness and cyber incident response have been developed at federal, state, and local levels of Government. Currently, there are multiple initiatives within NYC to engage volunteer cyber responders. Initiatives such as the NYC Cyber Critical Services and Infrastructure (CCSI) Project[109] - a formal partnership between the Manhattan D.A.'s Office, NYPD, NYC3, and the Global Cyber Alliance - or New York City Metro InfraGard Incident Management SIG[110] - a collaboration between the FBI and the private sector - are worth mentioning."

For NYC3 to create a network of cyber resources that is available during a cyber incident and able to scale quickly, NYC3 should explore mutual aid agreements with other jurisdictions. This could help address potential capability gaps without investing in new resources. For example, cyber volunteers can be redeployed from other existing initiatives like the National Guard. Hurricane Sandy has demonstrated how coordination before an emergency occurs can play a critical role when disaster strikes.

[109] New York Launces a Cybercrime Brigade, https://www.globalcyberalliance.org/new-york-launches-a-cybercrime-brigade/

[110] New York Metro InfraGard Members Alliance, https://www.nym-infragard.us/index.html.

DEFINING A MATURITY MODEL FOR CYBER VOLUNTEER STRUCTURES

In response to NYC3's request to construct a maturity model to assess the operations of a volunteers' corps, we developed the following comprehensive model to be used as a guide in the establishment of a volunteer corps. First, we define eight parameters drawn from the case studies analysis and from additional research on volunteers' challenges and benefits. We present the reasoning behind each of the parameters' importance for the evaluation of maturity and its contribution to the overall model assessment.

In the second part of this section, each parameter is assessed according to three levels of maturity: 'Basic,' 'Foundational,' and 'Advanced.' For each parameter, we offer a definition of each maturity level is provided in terms of readiness, that an emergency response volunteer corps could be assessed. The cumulative model will allow, in the future, comprehensive analysis and thorough assessment of a volunteer corps.

Maturity Model – Parameter Definitions

Augmentation Needs & Volunteer Corps Mission

Identifying the area of operations in which volunteers will be needed to augment existing response capabilities and defining a clear mission for the corps is a first step for the design and operation of an Emergency Response Volunteer Corps (ERVC).

Augmentation needs could result in reaction to a significant emergency incident that tested response abilities (e.g. Estonia CDU) or rather from a proactive approach taken to analyze emergency readiness and existing capabilities in advance of an incident. Taking the proactive path, such as in the case of NYC3, could improve an organization's response capabilities while avoiding the painful process of learning from mistakes. By analyzing capabilities and recognizing existing gaps, a volunteer corps will be well focused while targeting existing relevant needs. The mission of an ERVC will stem from the augmentation needs. A clear defined mission sets the tone for the rest of the building process and for the entire operation of ERVCs.

This parameter will be evaluated under two considerations: (1) clarity of defined needs and mission and (2) level of correlation between the two. The high correlation will allow the corps to put its operation focus where it is needed. We assess that the higher the correlation between the identified needs and the mission given to the volunteer corps the stronger will be the corps' foundations to build on. The next building blocks of the corps such as organizational, legal, or volunteers' engagement considerations would draw their focus from the strength of this parameter.

Identifying both augmentation needs and a clear mission should refer to stages in the CLC. The focus could be either on one stage of the CLC (e.g. only Response such as the MiC3 case), on several issues, or is meant to operate volunteers in the entire cycle. **We assume that focusing on one or several stages of the CLC does not impact maturity, as long as the corps is focused on its mission, to address existing needs.**

Organizational Parameters

Under two sets of organizational parameters, 'Framework' and 'Management' evaluate the organizational structure to support an ERVC. The wider the organizational support is, the higher will be the operating efficiency of a volunteers' corps. Under these parameters, the framework under which the corps is founded should be considered, as well as the resources dedicated for operation, designated management mechanisms, and the ability for periodical self-evaluation and additional external learning mechanisms.

Legal Parameters

Under two sets of legal parameters, the question that should be asked is how is the corps prepared for future possible legal obstacles resulting from volunteers' work? Answers will be provided by reviewing the supporting legal definitions and the coverage provided by law for the corps activities and specifically for volunteers' operations. We review the legal supporting framework in two directions (1) Legal authorities given for the operation of volunteers either to the corps or to the organization under which the corps is founded and (2) Legal coverage for the protection of volunteers operating under the corps.

Given the sensitivity of information sharing and access to crucial data systems, while defending from or responding to cyber threats, legal support is meant to protect both the operating organization and the volunteers from liability concerns. In addition, comprehensive legal assistance in the authorities given to the corps could mitigate trust issues that might challenge the ability of the corps to support cyber needs in the private sphere.

Volunteer Engagement

Under the next group of three parameters, we assess how the corps is prepared for the entire engagement process with volunteers over time, from an admission process perspective, training and implementation post-admission as well as incentive considerations meant to draw desired talent to volunteer.

Admission Process & Skill Set Definition

Under this parameter, we assess the volunteer's pre-approval processes. A structured admission process and a clear definition of skill sets required for the corps' activities could improve the readiness and maturity of EVRCs. From an admission process perspective, structure, and clarity matters. A structured screening process that includes, for example, preliminary tests and background checks for potential members, could create a more durable membership structure and performance.

From a skill sets perspective, to create a professional aptness between the potential pool of talent supplied by the market and expertise demanded by the cyber corps it is recommended to work with a recognized baseline standard. However, as there is currently no nationally accepted minimum qualifications credentialing system for cyber professionals, it is recommended to choose the skillset that best fit the environment in which the corps is operating. Many organizations, both public and private, have developed internal requirements for cyber professionals, which could be used as a benchmark for screening cyber first responders. Two such examples from the public sector that could be considered:

- The U.S. National Institute of Standards and Technology's (NIST) **National Initiative for Cybersecurity Education (NICE)** Cybersecurity Workforce Framework[111] – Common, consistent framework that categorizes and describes cybersecurity work, and is a reference guide to identify, recruit, develop, and retain cybersecurity talent.
- **DoDD 8570**[112] – Standards that apply to all personnel whose work relates to DoD information systems, requiring them to have training and certifications to be able to complete the minimum required skills. DoDD 8570 relies heavily upon a myriad of commercial certifications. Working with this standard will depend on the relevance of this training process to NYC3's needs, to match local systems and networks.

Training Structure & Implementation

From the post-admission perspective, we evaluate readiness for deployment of active members through ongoing training and deployment exercises. Both criteria are a part of the assessment of the preparedness of volunteers for action. Active deployment increases preparedness levels of a corps, and if appropriately debriefed could function as a measurement similar to exercises. Levels of cooperation with other main actors or with similar volunteer corps also provides insight into the strength of ongoing training programs.

Strong and Active private-public cooperation in both training and exercise is especially relevant. The private industry is an important partner in times of cyber crisis and therefore should be active in training implementation for cyber

[111] NIST Special Publication 800-181: National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework, https://doi.org/10.6028/NIST.SP.800-181.

[112] DoD Approved 8570 Baseline Certifications, https://public.cyber.mil/cw/cwmp/dod-approved-8570-baseline-certifications/.

emergency responders, as it might function both as a source for volunteers’ talent as well as a potential client for the corps deployment.

Incentives

Given ERVCs are dependent on volunteers' talent and their willingness to contribute their time and energy for the cause, assessing the level of 'attractiveness' of the corps, both in terms of monetary and non-monetary incentives, will provide more information on the ability of the corps to recruit excellent talent effectively. An incentive program is assessed by addressing both volunteers and their employers (if employed) considering the benefit of employers' support of volunteer's participation in the program. As one of the parameters to assess 'attractiveness' would be volunteers' satisfaction rates, the effectiveness of an incentives program will be best evaluated over time.

The topic of attractiveness is especially important, given that an enormous amount of talent lies in the private sector, usually within environments providing high levels of compensation. Professional training and networking options might be considered to be attractive for cyber volunteers, as well as access to advanced systems such as the cyber range. However, a cyber volunteer program should adapt its incentives to the environment in which it is active to be considered attractive for local cyber-professionals wanted as volunteers.

Maturity Model Layers

Parameter Assessment – Three Levels of Maturity

- In the model below, for each of the parameters, we defined three levels of maturity- Basic, Foundational and Advanced, according to the level of preparedness and readiness of the volunteer program in each separate aspect.
- The individual levels of maturity presented below were created from a careful analysis of existing volunteers' programs, both in the cyber sphere and in other realms, in addition to previous experience with volunteers in various programs.
- This model offers guiding tools for implementation for various volunteer corps. The structure is provided here, but the details of each program will have to be decided separately, tailored to the specific needs defined in the early steps of the process.
  - For example, programs focused on emergency deployment, such as MiC3, will implement the framework provided below differently than a city-led cyber corps that will use volunteers in various phases of the CLC.

	Maturity Model – Emergency Response Volunteer Corps			
		Basic	**Foundational**	**Advanced**
1	**Augmentation Needs & Volunteer Corps Mission**	A general definition of the need for augmentation in the emergency response process, no clear identification of a gap in capabilities, leading to a broad definition of the corps' mission. *(no explicit reference to CLC)*	Identification of evident augmentation needs in the CLC that a volunteer corps could fulfill (either learning from experience or through proactive review & analysis of emergency needs). Clear and specific corps' mission defined, addressing phases of emergency response. *(identify needs by CLC)*	Foundational + High correlation between the identified augmentation need and the corps' defined mission
2	**Organizational** **-** Framework	Corps founded under the home organization's existing organizational structure No separate organizational framework for operating volunteers.	Basic + - Organizational chart, designated roles for volunteers - Clear budget allocation and long-term budget planning for the corps - **Internal audit**: once a year / other method for self-evaluation mechanisms	Basic + Foundational + **External audit**: The effectiveness of the Corps' plans is continuously examined and improved through various opportunities and demonstrated for the public interest, with structured external processes in place.
3	**Organizational** **-** Management	**Ad-hoc management** of the team evolving around the admission process, recruitment, and deployment.	An existing **mechanism** for maintaining the volunteer squads' activity in terms of their skills, credentials, clearance, participation, etc. The corps' activities are based on formulated management and operational plans: clear allocation of volunteers to missions/teams, with an existing process for team building over time.	Basic + Foundational + Designated Program Manager/volunteer coordinator managing both professional & administrative volunteer needs
4	**Legal-** Authorities	Volunteers are acting under existing authorities given to 'home organization,' no specific legal reference for volunteers' work in the organizations' legal definitions.	Authorities to operate volunteers are given to 'home organization' and defined under legal definitions.	**Full designated legislative support for the corps activities to address any liability concerns:** 1- Clear authority to deploy volunteers by law is given to the corps/home organization. 2- Clear legal cover for volunteers' operations, including specific protection

	Maturity Model – Emergency Response Volunteer Corps			
		Basic	**Foundational**	**Advanced**
5	**Legal-** Volunteers' Protection	Partial or non-comprehensive protection of possible liability issues Internal agreements/Terms of reference/rules of engagement between the organization and the volunteers	Acting under existing volunteer protection legislation: General / non-cyber-specific protection on volunteers	related to the volunteers' work. **Level of legislation (EO/ city / state legislation) - TBD according to existing needs.** *(cyber-specific protection for both organization & volunteers)*
6	**Volunteers Engagement-** Admission Process & Skillset Definition	**Structured admission process**: preliminary admission exams process, minimum certifications & work experience requirements, background/criminal check, a commitment of the volunteer, employer agreement (if necessary).	Basic+ The clear and full definition of skillset required in the admission process. Skillset required matches the corps mission, with clear allocation of skill sets to corps assignments.	Basic + Foundational + Skills standard adopted *(match NIST NICE Cybersecurity Framework / DoD standards / another relevant standard)*
7	**Volunteers Engagement-** Training Structure & implementation	Professional training relying solely on volunteers' previous training & experience.	Structured internal training program for volunteers upon arrival and throughout their membership + Timely exercises (at least 2 per year) / active deployment (1 per year)	Basic + Foundational + Active private-public cooperation in training, structured in the annual exercise program. Professional learning mechanism cooperating with other existing programs (corps or others).
8	**Volunteers Engagement-** Incentives	Providing ad-hoc incentives for volunteers without structured, developed incentives programs. No specific budget allocation (Ex: only network opportunity within the community)	Basic + - Clear budget allocation for training programs, networking events, maintaining active communication of the group. - Developed incentives for employers, developing private-public cooperation	Basic + Foundational + - X% satisfaction rate of volunteers from the program - The number of professionals interested is higher than the demand. - Proven satisfaction of volunteers over time- X number of 'dropouts' from the program (X defined by the host organization according to experience and the given environment).

Table 2. Maturity Model - Emergency Response Volunteer Corps Table[113]

[113] Created by SIPA Capstone Project Team based on research.

KEY FINDINGS & RECOMMENDATIONS

Throughout the process of researching designs for a volunteer cyber corps for NYC3, our team identified the following as critical pillars needed to support the formation of a volunteer cyber corps: sufficient legal liability protections and incentivizing NYC's sophisticated workforce to participate. As such, our below final recommendations consider findings made from the case studies as well as those uncovered during the above analysis into legal considerations and how to motivate and incentivize volunteer participation.

Additionally, as experience shows, failing to plan for emergency events is a plan for failure. For example, following Hurricane Sandy, more than 900 people from New York's startup community signed up to help. Still, a lack of coordination prevented them from getting involved.[114] This suggests that the necessary volunteer expert talent exists, but is not being utilized. To develop a resilient and capable volunteer corps, NYC3 should implement a set of essential steps, described in the section above, "Defining a Maturity Model for Cyber Volunteer Structures." The essential steps and components of volunteer corps are summarized in the below table and subsequent recommendations:

Planning	Recruiting	Training	Managing	Evaluating
Conduct Organizational Needs Assessment	Find Volunteers	Induction Training	Supervise Volunteers	Evaluate Volunteers
Identify Volunteer Roles	Screen Volunteers	Professional Development Activities	Cultivate Sustainable Volunteer Corps	Evaluate the Volunteer Program
Develop Job Descriptions	Get Employee / Employer Approvals		Regular Communication	Report Results
Assign/Hire Volunteer Coordinator	Conduct Orientation		Recognize Volunteers' Efforts	

Table 3. Summary Program Stages & Recommendations[115]

[114] "*The Nerd Reserves: Sandy Recovery Renews Call For Tech National Guard*," Gerry Smith, November 21, 2012, https://www.huffpost.com/entry/tech-national-guard_n_2168374.

[115] Created by SIPA Capstone Project Team based on research.

Define the Scope of NYC3's Volunteer Cyber Corps

- **Recommendation**: Conduct an organizational needs assessment driven by a gap analysis of existing staff and staffing plans.
  - Because we recognize that volunteers can provide a value-add throughout the cybersecurity life cycle, such as working on education initiatives in the 'Protect' phase, we believe NYC3 must conduct a needs assessment and gap analysis to identify areas in which capacity is either underdeveloped or has the potential to be overwhelmed during a cyber incident.
- **Recommendation:** Create a clear mission statement for the program that speaks to the goal of a volunteer cyber corps.
  - As part of the need's assessment process, NYC3 should develop a mission statement for the program that clearly articulates the objective of a volunteer cyber corps to draw in talented cybersecurity professionals and highlight the importance of the organization to the daily lives of New Yorkers.
- **Recommendation:** Provide prospective volunteers with well-defined roles and responsibilities.
  - NYC3 should provide prospective volunteers with a clear set of roles and responsibilities. This is a critical step to begin driving participation by illustrating the notion that the work at the volunteer-level is important and, depending on the phase they're involved in, only open to individuals with the proper skill sets and qualifications.

Solidify Volunteer Program Framework & Design

- **Recommendation**: Assign dedicated volunteer management.
  - Drawing on examples from previous cases, we believe that assigning or hiring a dedicated volunteer manager is essential to the overall effectiveness of a volunteer corps. What's more, dedicated staff resources should be responsible for all volunteer communication and outreach as well as training opportunities for volunteers alongside coordinating general activity.
- **Recommendation:** Develop a systematic approach to volunteer inclusion and selection.
  - Because cyber volunteers could be involved throughout all phases of the cybersecurity life cycle, it is imperative that NYC3 screens for skills needed in every phase. This includes an approach to volunteer selection and screening that adequately identifies qualifications needed from prospective volunteers depending on the role in which they're applying. For example, if a volunteer is applying for a position in the 'Identify' phase, it could be helpful to ensure candidates have experience with malware analysis and detection.
- **Recommendation:** Establish clear and open lines of communication with volunteers.

- Once volunteers have joined the program, dedicated staff must ensure that lines of communication are open at all times. This is because volunteers could be needed at short notice or on an ad-hoc basis.

Create an Approach to Volunteer Engagement & Outreach

▶ **Recommendation:** Implement a volunteer engagement strategy that includes a detailed screening process, outlines potential volunteer pools, and explores incentives NYC3 can offer.

- We believe that it is important for NYC3 to spend time highlighting potential sources of volunteers to create the basis of an outreach strategy. For example, depending on skill sets needed, NYC3 may need individuals with Cobalt programming experience, which could be found in the retired cyber professional community.
- Volunteer opportunities that maximize the skill sets of volunteers, and are seen as scarcer than other ways to give back to a community, are more successful at drawing talented candidates. Additionally, research has shown that cyber professionals specifically are more likely to participate in volunteer programs when training components are included that bolster their own skill sets alongside potential networking opportunities.

▶ **Recommendation:** Leverage existing relationships with private sector companies to gain access to volunteers.

- To broaden its volunteer pools, NYC3 should adopt an engagement strategy that leverages its existing relationships by seeking volunteers from multiple organizations rather than drawing from one volunteer pool. If volunteers are predominately from one sector and impacted by a cyber incident, employers may require their attention; rather volunteers could be distributed across sectors or industries to provide elasticity to the program.

▶ **Recommendation:** Seek employer approval for prospective volunteers.

- During a cyber event, our research has shown that volunteers may be needed by their employers if they're impacted as well. Additionally, in blue-sky days, volunteers will need dedicated time to attend training and general interaction with NYC3. For these reasons, as well as drawing on examples from other programs, such as MiC3, we believe it is important that NYC3 obtain employer approval for volunteer participation as part of the application process to volunteer for NYC3.

Address Legal Considerations

▶ **Recommendation:** Review and update legal coverage for volunteers and deploying agency NYC3.

- Because volunteers may participate in all facets of the cybersecurity life cycle, it is important to ensure that, depending on their role, volunteers and their deploying agency are adequately protected from issues of legal liability. For example, if volunteers are asked to take a more hands-on-keyboard role they may need more protection than if they were instead focused on education and community outreach.

- **Recommendation:** Codify the existing executive order through the City Council or New York State
  - As a first step to protecting volunteers from issues of liability, NYC3 should evaluate legislative codification of the executive order that underpins its authority through City Council. We believe taking this step, in the absence of a "good samaritan" style law with specific carve-outs for cyber volunteers, is important to confirm adequate legal protection to NYC3's cyber volunteer corps.

APPENDIX

Appendix 1 – Key Contributing Factors (Excerpt) of Volunteer Retention and Recruitment Problems Identified by the USFA's Research

- **Management Style:** Many volunteers have been driven out by problems with their chief or officers' management style, resulting in a move toward participatory management. Volunteers have a lot to offer and must be used effectively, or they will be lost.
- **Mission Statement:** Emergency service organizations must understand "where they are" and "where they are headed." It is, therefore, important to plan the way into the future by developing a goal, mission, objectives, and vision.
- **Training of the Chief and Officers:** Officers need to take classes in leadership and acquire the skills of directing personnel and managing a group composed of all age levels. Chief level officers, in particular, should take additional courses in volunteer management and leadership such as the USFA National Fire Academy's Volunteer Incentive Program, which is a free training program. Officer training must be affordable, accessible in the field, scheduled on nights and weekends, and conducted in a period "that works."
- **Internal Communications:** The vast majority of management problems are due to miscommunications, misinformation, or wrong assumptions by members. These problems can be avoided by providing regular "good information" to members through formal discussions, postings, emails, and newsletters that are open and available to all members.
- **Volunteer Coordinator:** The purpose of the coordinator is to assist with many of the day-to-day tasks of running the department such as scheduling training classes and processing paperwork, to improve coordination of day-to-day activities by serving as a liaison between volunteers and the fire chief, and thereby to relieve the officers of the burdens of running the department. A volunteer member may fill this position, but in large or busy systems, it is preferable to establish this as a career position due to the volume of work.
- **Delivering Public Fire Safety and Prevention Programs:** In addition to their importance for fire safety, public education and prevention activities improve the visibility and image of volunteer departments. These activities may include displays at public locales, fire, and public safety classes, and performing drills in schools.
- **Use of Media:** With proper exposure through the media, a fire department can garner financial and moral support for its volunteers. Remember, however, that the media likes controversy, and may play up problems within the department.
- **Working with Local Politicians:** To maintain political support, work closely with local political leaders to make sure they understand what the fire department does and the level of dedication of volunteers. Departments should work closely with politicians to acquire incentives for their members and discuss benefits for companies or businesses that will allow volunteers to respond from work.

- **Liability Coverage:** Fear of being sued and losing personal assets exists among some members of the volunteer fire service despite many legal protective clauses such as the Good Samaritan Act to protect volunteers. Some departments give members a pamphlet outlining the major issues of liability for a volunteer firefighter. Others recruit a lawyer or member to help protect them from liability issues by, for example, providing advice on ways to reduce liability exposure. If the department believes that there is a potential risk for members to be sued, it should purchase liability insurance for itself and its members.
- **Non-Firefighting Personnel:** Fire departments offer a variety of support positions such as bookkeeping, data management, fundraising, fire prevention, public safety education, public information, building maintenance, and apparatus maintenance that can be filled by people who are not firefighters and who do not respond on calls. The role of administrative and non-firefighting members is crucial because, without them, firefighters might leave the volunteer service due to the burdens of paperwork or fundraising.
- **The Dilemma of Reducing Training Requirements:** Today's training standards have increased professionalism and safety, but also created a major barrier for recruitment and retention because the requirements are very time demanding. Basic training is needed to ensure that firefighters know how to perform certain tasks safely and efficiently. However, training standards should not be set so high that they discourage volunteerism.
- **Training in Context:** Training is not perceived as a burden if it is wanted. To be wanted, training must be on topics considered important to the volunteer, and it needs to be well-presented, progressive, and include student involvement and activities. Training in context, which uses specific operational scenarios, and provides more realistic training, allows students to combine skills they learned in a basic firefighting class into a mock scenario.
- **Duty Shifts:** Duty shifts help retention by limiting time demands placed on volunteers. Volunteers are on call or in the station only during assigned periods. Duty shifts remove the burden of having to be available 24/7. A drawback of using shifts is that the total number of members may have to be increased to have enough staffing for each shift. The shift system also may require spending money on additional equipment and insurance.
- **Handling the Most Demanding Hours:** Weekdays are generally the most difficult periods for volunteers because most members are at work. One way to address the weekday staffing problem is to recruit members who work at night but are available during the day.
- **Recognition:** Most volunteers want to be appreciated for their service to the community. Recognition can be by awards or as simple as a pat on the back or a picture in the local paper.

- **Setting Up an Incentive System:** The most successful incentive programs today are diverse and appeal to volunteers of all ages, experiences, and ranks.[116] Fire departments should not limit themselves to one type of incentive program for all volunteers because one program may not appeal to all members. Each item on the menu should provide similar benefits so that volunteers who choose different things receive identical benefits. The benefits of retaining members by providing small financial incentives far outweigh the costs of excessive turnover or hiring full-time firefighters.
- **Recruitment Coordinator:** Most departments prefer formally appointing an individual to serve as the department's focal point for recruiting. The coordinator can orchestrate recruitment by all members, conduct a membership needs assessment, formulate recruitment messages and materials, do some of the recruiting directly, and arrange for others to help, and interview prospective members, and answer their questions.
- **Tests and Background Checks:** It is recommended that combination departments require all volunteers to pass the same written, physical agility, and health exam given to career members. Most departments have established relationships with local law enforcement officials to review an applicant's driving and criminal record. Application forms often ask the applicant to agree to driving and criminal checks. Failure of applicants to agree to the checks may be cause for not accepting them. Some departments also refuse people convicted of driving while intoxicated within the past five years, or at a minimum, allow these individuals to join but restrict them from driving department vehicles.
- **Commitment Agreements:** Fire departments may request that new members sign a commitment agreement, which aims to lay out expectations on paper so that there is no misunderstanding about what the department is asking them to do.[117] Commitment agreements are generally nonbinding because the members are volunteers.

[116] See U.S. Fire Administration, "*Retention and Recruitment for the Volunteer Emergency Services: Challenges and Solutions*," May 2007, https://www.usfa.fema.gov/downloads/pdf/publications/fa-310.pdf, 100-112 for actual examples of incentives used to recruit and retain volunteer firefighters and EMS personnel, such as direct and non-direct monetary ones. See also Ibid., 112 and 114 for sample award tiers point system in those incentive programs.

[117] See Ibid., 154 for a sample commitment agreement.