Pen Testing a City

Gregory Conti (West Point), Tom Cross (Drawbridge Networks),
and David Raymond (Virginia Tech)

Abstract

How would you take down a city? How would you prepare for and defend against such an attack? The information security community does a great job of identifying security vulnerabilities in individual technologies and penetration testing teams help secure companies. At the next level of scale, however, things tend to fall apart. The information security of cities, the backbone of modern civilization, often receives little to no holistic attention, unless you count the constant probing of nation state aggressors. The information technology infrastructure of cities is different from other entities. Cities feature complex interdependencies between agencies and infrastructure that are a combination of federal, state and local government organizations and private industry, all working closely together to keep the city as a whole functioning properly. Preparedness varies widely. Some cities have their act together, but others are a snarl of individual fiefdoms built upon homegrown technological houses of cards. If you can untangle the policy and politics, and overcome the bureaucratic infighting to create workable leadership, authorities, and funding, you are still faced with an astronomically complex system and an attack surface the size of, well, a city. Our work identifies these necessary precursor steps and provides a broadly applicable set of tools to start taming and securing such an attack surface.

1. Introduction

Security is hard. Even in small organizations with well-understood network infrastructures, keeping intruders out cannot be guaranteed. Imagine a large, diverse infrastructure where a variety of bureaucracies and critical infrastructure components share complex interconnections with, perhaps, no overarching cybersecurity architecture. This is what your city probably faces.

Cities are fragile even in the best of times, that is, when nobody is actively trying to subvert critical infrastructure or other important systems. Examples abound of cascading failures caused by system malfunctions, natural disasters, or industrial accidents that result in city-wide disruption, and sometimes even chaos. One example is the 1977 New York City blackout, caused by two lightning strikes at a power substation in Buchanan New York on July 13th of that year. The strikes started a series of failures that resulted in a 2-day blackout. Looting, vandalism, and arson were widespread when the thin veneer of civilization was torn away by the brief loss of power. Over 1,600 stores were damaged and NYC fire stations responded to over 1,000 fires. Almost 4,000 people were arrested and packed into overcrowded jail cells. Imagine what might happen if someone were actively *trying* to cause systems to fail; perhaps over a long period of time. It is not hard to imagine future scenarios like the New York City blackout, or worse.

In this paper, we first examine an existing penetration testing framework and propose how it might be extended for a city-level penetration test. We then deconstruct a notional city layer by layer, and use these insights to suggest a comprehensive methodology for reverse engineering any city and deriving its attack surface. We complement these insights with a broad analysis of proven capabilities demonstrated by hacker and information security researchers as well as known capabilities of criminal and nation-state actors applicable to city-level attacks. Finally, we conclude with a wide-ranging set of approaches to complement pen testing efforts, including exercises and collective training, metrics and a maturity model for measuring progress, and specialized city-level attack/defend ranges. This paper will, perhaps, leave you fearing for the survival of your respective country, but also possessing a toolkit of techniques to help improve the situation. By better securing cities we have a glimmer of hope in securing nations.

2. Penetration Testing

The SANS Institute has been teaching a standardized penetration testing process for years in their Security 560: Network Penetration Testing and Ethical Hacking course. Their basic process is the following[1]:

1. Preparation
   a. Sign Non-disclosure Agreement (NDA) and receive signed permission memo
   b. Agree on scoping and Rules of Engagement (ROE) with target company
2. Testing
   a. Conduct open-source reconnaissance on the target company and network
   b. Conduct IP and port-level scanning to identify outward-facing services and potential vulnerabilities
   c. Exploit target network using targeted exploits against discovered vulnerabilities
   d. Conduct password attacks against compromised hash files
   e. Assess and attempt to compromise wireless infrastructure
   f. Assess and attempt to compromise web applications
3. Conclusion
   a. Analyze results and retest as necessary
   b. Provide detailed penetration test report and presentation

This methodology is designed to assess a corporate network, but likely does not scale well to a city's infrastructure. A city-scale penetration test must necessarily begin with a broad analysis of the audit surface at multiple layers of abstraction to determine all potential attack vectors before the rest of the process can begin. Below is a more robust process that can be executed at the city level.

1. Preparation

[1] Adapted penetration testing process from SANS Security 560, V2010_1226, book 1, pages 55-56.

    a. NDA/permission memo
    b. Define “City” (Scope)
2. Determine audit surface area at each level of abstraction
    a. Determine how to collect information at each level
3. Cross sectional analysis
4. Pressure point analysis
5. Risk analysis of threat actors
    a. Most likely courses of action
    b. Most dangerous courses of action
6. Conclusion
    a. Analyze results and retest as necessary
    b. Provide detailed penetration test report and presentation

In the following sections, we examine the various components of this city-level penetration testing process in more detail.

3. Dissecting a City and Determining the Audit Surface

Cities come in various shapes and sizes and there are no strict rules to dictate a municipality’s qualification as a city. Dictionary.com defines a city as an “incorporated municipality, usually governed by a mayor or council.” Wikipedia goes on to qualify a city as having “complex systems for sanitation, utilities, land usage, housing, and transportation.” To be a relevant target for a penetration test, a city must have a network that incorporates municipal infrastructure components and that could be a target for someone who might want to disrupt city operations.

Cyberspace Planes.

To understand how a city’s information technology infrastructure is organized, it is helpful to break it down into the cyberspace planes[2] shown in figure 1. At the bottom is the geographic plane, at which resides the physical location of IT systems or devices. While physical location is not always relevant, in the case of a flood or other natural or man-made disaster, physical location can be very important. Up one plane is the physical, which is essentially the physical layer of the Open Systems Interconnect (OSI) model. At the logical plane are layers 2 (link) through 7 (application) of the OSI model and includes all operating systems and application software, as well as network protocols and device drivers. At the cyber persona plane are accounts that are associated with individuals or groups. Finally, the supervisory plane includes persons, organizations, or systems that provide command and control.

[2] David Raymond, Gregory Conti, Tom Cross, and Robert Fanelli. "A Control Measure Framework to Limit Collateral Damage and Propagation of Cyber Weapons." International Conference on Cyber Conflict (CyCon), Tallinn Estonia, June 2013.

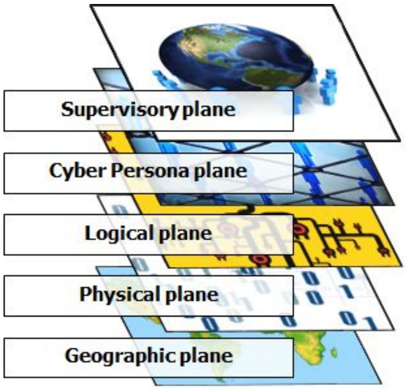


Figure 1. Cyberspace planes.

In a city-level IT infrastructure, the supervisory plane can be particularly complex as a result of the potentially contentious political atmosphere. Even if the politicians get along, it is often the case that each is working to further their particular agenda and make themselves look good to voters, notwithstanding the challenges they might be creating for IT security staffs. For example, some large cities have large police and fire departments, whose leadership have significant political clout. The municipality's organization chart might show these Police and Fire Chiefs beholden to the Mayor or City Manager, but in reality they may be at liberty to ignore cybersecurity directives coming from City Hall. This is just one example of the potent complexities of small town (or big city) politics. The supervisory plane in a city might also be prone to compartmentalization between the siloed infrastructure sectors, further hampering security cooperation.

Below the supervisory plane is the persona plane, which includes online identities of municipal leaders and employees. These personas might be shared freely online to demonstrate openness and to welcome voter interaction. This kind of openness might provide a political boost, but it also invites spear-phishing and other scams. At the logical plane, there are likely incompatibilities between software systems that keep various sectors functioning. In fact, many might run on legacy hardware and software, owing to regulatory requirements and/or the expense of upgrading. The physical plane might be hampered by low-bandwidth connectivity and a lack of redundancy in physical-layer connectivity. The geographic plane can be particularly important to city services. While corporations can have branch offices and widely distributed network operations, a city IT infrastructure is generally tied to the geographic area of the city. Localized natural or man-made disasters could easily result in loss of power or loss of network connectivity.

What makes a city different?

In some ways, a city can be treated like a company when scoped for a penetration test. A city can usually be partitioned into business units, each with it's own strengths, vulnerabilities, and priorities. As is true in most companies, cybersecurity is a cost center, draining assets while not contributing to the overall functioning of the municipality. Unlike a company, budgets are often severely limited and there are complex legal authorities that can impact who can dictate requirements for different infrastructure components. For example, rules governing networked devices used in hospitals and other healthcare settings are likely to be dictated by the Food and Drug Administration, severely limiting the influence that a city-level information security officer can have on them. Other critical infrastructure sectors likely fall into similar situations, with the DOD governing defense industrial networks, the Federal Energy Regulatory Commission overseeing electrical power infrastructure, and the US Department of the Treasury governing financial services. This leads to much more complex legal and regulatory frameworks within which security professionals must operate.

Confounding these already existing challenges are various “smart city” initiatives that strive to make cities more efficient through improved interconnectivity. Like many new IT systems, these initiatives often ignore, or at least de-emphasize, security as they strive for functionality and interoperability. Examples include Cisco’s Smart+Connected Communities[3], IBM’s Intelligent Operations Center[4], and Google’s Sidewalk Labs[5]. These well-meaning efforts nevertheless make life more difficult for those trying to secure a city’s infrastructure.

4. Cross Sectioning and Pressure Point Analysis

Each city is has a different mix of the various critical infrastructure sectors, making each of their attack surfaces different. A center of gravity (COG) analysis is helpful in identifying a city’s specific areas of vulnerability. The center of gravity is a concept borrowed from military doctrine. The Department of Defense defines a COG as “the source of power that provides moral or physical strength, freedom of action, or will to act[6].” The center of gravity is, therefore, usually seen as the source of strength. Originally used to assess enemy military units, the COG analysis has been leveraged with great success on metropolitan areas during the recent conflicts in Iraq and Afghanistan to help military units identify where to focus their efforts when trying to help a local population improve the standard of living in their communities. This same concept can be used to assess areas of concern and to focus efforts during a city-level penetration test.

One example of a city COG is the financial sector in New York City. Anyone trying to bring NYC to its knees would do well to attack the financial sector, which is a significant source of the city’s strength. In Houston, TX, oil and other energy companies would be seen as a COG, while in Las Vegas, the gambling industry is an obvious COG. During a COG analysis, it is also important to consider “non-critical” sectors, such as churches, libraries, sports facilities, local banks, law offices, schools, and others. Some of these might be as important to the local

[3] http://www.cisco.com/web/strategy/smart_connected_communities.html

[4] http://www-03.ibm.com/software/products/en/intelligent-operations-center

[5] http://sidewalkinc.com/

[6] Department of Defense. Joint Publication 1-02, Dictionary of Military and Associated Terms, 8 Nov 2010 (as amended through 31 Jan 2011).

communities as critical infrastructure sectors or major industries. An analysis of the interdependencies between these entities follows from the COG analysis and can provide interesting insights into how the city as a whole might respond to a major breach in one particular sector. Further discussion on current research into interdependencies between infrastructure sectors is given below. While this work is helpful, it is incomplete as it does not address other potential centers of gravity.

5. City-level Vulnerability Research

To understand the potential vulnerabilities that cities might face, it is helpful to review previous research into systems that make cities function; systems such as traffic control, road signs, elevators, power meters, water, power, and toll collection. This section provides a brief survey of this research.

Portable electronic road signs can easily be subverted to display any desired text. The controls are located within the sign and even if the operators change the (simple) default password, a simple factory reset will restore it to the default[7].

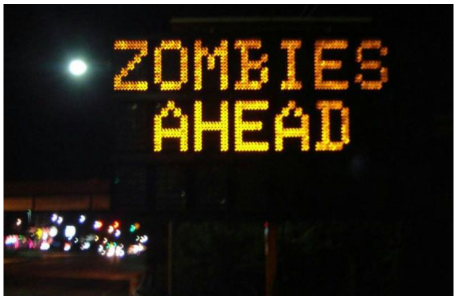


Figure 2. Portable road signs can be used to divert traffic, or for other nefarious purposes.

In 2013, malicious hackers caused emergency alert systems throughout the country to signal bogus ‘disasters’, interrupting local televising programming and sending false alerts[8].

Wireless traffic control systems are a growing trend. Most are installed using simple sensor networks and many are woefully insecure. In a DEF CON talk in 2014, Cesar Cerrudo from IOActive Labs showed how many wireless traffic control protocols are easily subverted, causing traffic lights to bend to the will of the attacker[9]. Cesar has demonstrated that this hack works in cities worldwide, including major cities in the United States.

Modern high-rise buildings would not be possible without Elisha Otis’ 1852 invention of the ‘safety elevator’, which used a brake system to prevent disaster in the event of a lift cable failure. Recent research has shown, however, that elevators are rife with technical and

[7] http://jalopnik.com/5141430/how-to-hack-an-electronic-road-sign

[8] http://www.ksl.com/?sid=24061333

[9] http://blog.ioactive.com/2014/04/hacking-us-and-uk-australia-france-etc.html

systemic security flaws. It is not surprising that elevator banks are controlled by common Industrial Control Systems (ICS), many of which are notorious for running on legacy systems with infrequent (or nonexistent) patching. Fire safety regulations also require that elevator banks be controllable using uniform elevator keys. These keys are often the same state-wide and using a key switch on the first floor (or other designated landing), must be able to put any elevator bank in fire service mode, putting all elevators out of service until fire safety mode is turned off. Another key used inside elevator cars allows someone with a fire safety key to control the car independently. Many of these fire safety key biting codes (key patterns) are included in downloadable fire safety regulations. Imagine putting banks of elevators in large building out of service with the turn of a key.

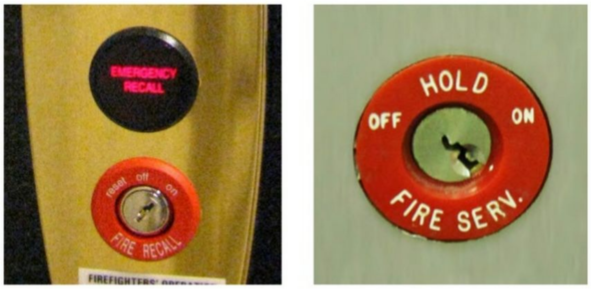


Figure 3. Elevator fire service key switches.

Major hacks against Saudi Aramco in 2012[10], and against the the Sands Casino[11] and on Sony Pictures Entertainment[12] in 2014, are examples of attacks on industries that could have far-reaching consequences on a city if they were coordinated with infrastructure attacks.

The potential for attacks at airports abound. From vulnerable Internet kiosks[13], to well-publicized TSA security gaps[14,15], to constant reports of fence jumpers[16]. A well coordinated attack on an airline hub such as Denver or Atlanta could impact air traffic nationwide.

6. Analysis

The threat posed to a city by the vulnerabilities outlined above are dictated by the ability and intent of an adversary. By replicating the work of security researchers, an unsophisticated adversary could easily cause localized disruption by compromising wireless traffic control

[10] http://www.theregister.co.uk/2012/08/29/saudi_aramco_malware_attack_analysis/

[11] http://money.cnn.com/2015/02/27/technology/security/iran-hack-casino/

[12] https://en.wikipedia.org/wiki/Sony_Pictures_Entertainment_hack

[13] https://www.youtube.com/watch?v=dxWl8bMCThs

[14] https://www.youtube.com/watch?v=KON9TYh5_xk

[15] http://www.forbes.com/sites/danielreed/2015/06/08/the-tsas-95-failure-rate-be-carefull-what-you-ask-for-when-demanding-that-congress-do-something/

[16] http://www.scpr.org/news/2015/04/09/50907/ap-investigation-dozens-of-intruders-have-breached/

systems or a large building's elevators. More widespread disruption would require multiple simultaneous attacks, possibly across multiple sectors. This would require a higher level of attacker sophistication, or at least close cooperation between multiple small-time actors. True chaos requires an understanding of the interconnectivity between the different critical and non-critical infrastructure sectors, and between centers of gravity discussed previously. As a defender, understanding and mitigating these interdependencies can go a long way toward preventing large-scale disruption of a metropolitan area.

An example of the cascading failures that disruption in one infrastructure sector can produce on others is the derailment of a commuter train in Baltimore's Howard Street Tunnel in 2001[17]. This derailment caused expected effects in train and automobile traffic. It also caused a water main break, which led to localized flooding, causing power to be knocked out in much of downtown Baltimore. Fiber optic cables in the tunnel were destroyed, resulting in major disruption in phone and Internet service that affected several corporate headquarters including WorldCom, Verizon, the Hearst Corporation (in New York City), and Nextel. Fortunately for security professionals, a body of work on interdependencies between infrastructure sectors already exists in the scientific literature. A comprehensive survey of international research on interdependency modeling was prepared by researchers at Idaho National Laboratory in 2006[18]. Figure 4 illustrates one way to visualize interdependencies between sectors, in this case for a flooding event such as 2005's Hurricane Katrina, which had a devastating impact on New Orleans and other parts of southeast Louisiana[19]. In the figure, individual infrastructures are represented on a single plane, parallel lines represent subsets of an infrastructure, nodes represent key infrastructure components, and dotted lines indicate interdependencies.

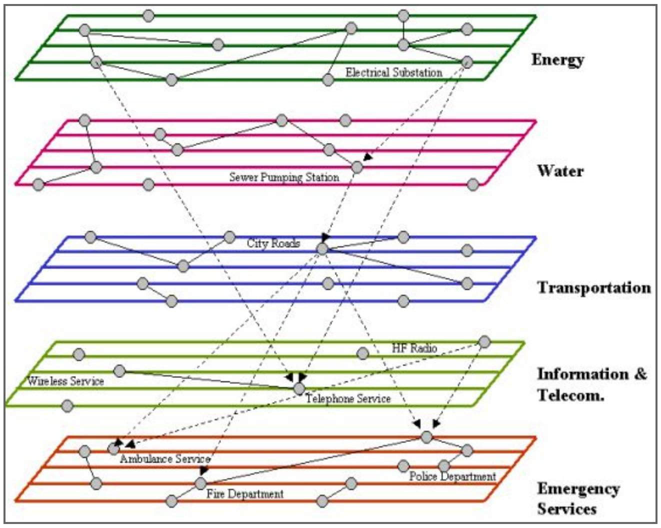


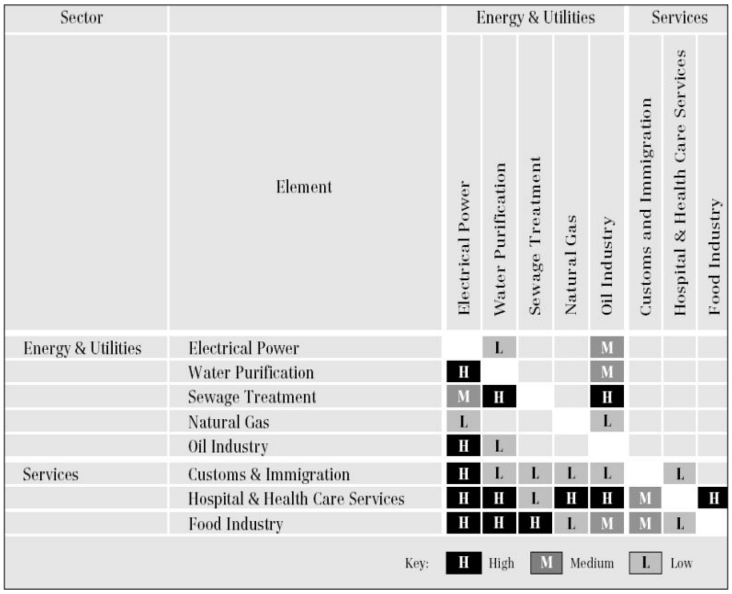
Figure 4. Interdependency Modeling (Flooding Event).

[17] P. Pederson, et al. Critical Infrastructure Interdependency Modeling: A Survey of U.S. and International Research. Online. Available at http://www5vip.inl.gov/technicalpublications/Documents/3489532.pdf. Aug. 2006.

[18] Ibid.

[19] https://en.wikipedia.org/wiki/Hurricane_Katrina.

Another way to visualize infrastructure interdependencies is the critical infrastructure dependency matrix shown in Figure 2, used by the Critical Infrastructure Protection Task Force of Canada.



Sector		Energy & Utilities					Services		
	Element	Electrical Power	Water Purification	Sewage Treatment	Natural Gas	Oil Industry	Customs and Immigration	Hospital & Health Care Services	Food Industry
Energy & Utilities	Electrical Power		L			M			
	Water Purification	H				M			
	Sewage Treatment	M	H			H			
	Natural Gas	L				L			
	Oil Industry	H	L						
Services	Customs & Immigration	H	L	L	L	L		L	
	Hospital & Health Care Services	H	H	L	H	H	M		H
	Food Industry	H	H	H	L	M	M	L	

Key: H High M Medium L Low

Figure 5. Infrastructure Dependency Matrix.

Most interdependency modeling is conducted in the context of natural disaster or terrorist event scenarios, however, the results map almost directly to potential cybersecurity scenarios. Examples of efforts and organizations that model interdependencies are the National Infrastructure Simulation and Analysis Center at Sandia National Laboratories[20] and the Multi-network Interdependent Critical Infrastructure Program for Analysis of Lifelines (MUNICIPAL), a cooperative effort between Rensselaer Polytechnic Institute and the National Science Foundation[21].

This interdependency research is currently limited to the critical infrastructure sectors, but it could be extended to include non-critical infrastructure and other city-level centers of gravity.

7. Solutions

Solving the security challenges posed by city-level technology systems requires support and buy-in from executive leadership, whether that be a mayor or city manager, and might also require the support of the city council. In this section, we describe a new initiative, Securing Smart Cities, and make recommendations for other solutions that city leadership should explore.

[20] http://www.sandia.gov/nisac/

[21] http://ascelibrary.org/doi/abs/10.1061/(ASCE)NH.1527-6996.0000182.

Security Smart Cities Initiative

One very promising solution to the myriad vulnerabilities in city infrastructure is the Securing Smart Cities Initiative[22], a not-for-profit initiative designed to help local governments secure their infrastructures. This initiative, spearheaded by the security research firm IOActive and their chief technology officer Cesar Cerrudo, is currently supported by organizations such as Kaspersky Lab, the Cloud Security Alliance, and the Institute for Critical Infrastructure Technology, among others. The Securing Smart Cities Initiative hopes to educate city planners and providers on the importance of security best practices, foster collaboration among partners to share methodologies, foster partnerships between cities, technology providers, and the security community, and develop standards, guidelines, and resources to help improve cybersecurity across all areas related to smart cities.

Other solutions proposed by the initiative include developing cybersecurity checklists for smart cities, promoting encryption, strong passwords, and structured patching regimes, tracking access to city systems, running regular penetration tests, forming and exercising emergency response teams, and creating manual overrides for all smart city systems.

Other Proposed Solutions

Some security solutions are common to any enterprise network. City-level Network Operations Centers (NOCs) or Security Operations Centers (SOCs) should be established (if not already present) and security teams should look into leveraging threat intelligence as part of their security infrastructure. Effective metrics for assessing the effectiveness and performance of security solutions are the only way to determine whether your security team is on the right track.

In addition to traditional security recommendations, cities must incorporate a robust analytic framework into their assessment process. Detailed center-of-gravity analysis, interdependency analysis, and threat analysis should be used together to help determine how breaches in one sector might impact other sectors. Meaningful city-level exercises, starting with tabletop events and progressing to more sophisticated simulations, can help inform security managers about the consequences of possible attack scenarios, and more importantly, can help to exercise incident response teams. SANS CyberCity[23] is a simulation environment that incorporates a scale model of a city with real-world supervisory control and data acquisition (SCADA) and industrial control systems (ICS) to give security professionals an environment to attack and defend a notional city. The Michigan Cyber Range's Alphaville[24] provides a similar environment, without the physical city model. Finally, computer games/simulations such as SIMCITY[25] have evolved to the point that they can simulate infrastructure interdependencies with reasonable accuracy and can be used to analyze these connections.

[22] http://securingsmartcities.org

[23] https://www.sans.org/netwars/cybercity

[24] http://www.merit.edu/cyberrange/alphaville.php

[25] http://www.simcity.com/

A capability maturity model (CMM) for city-level security integration could be an excellent tool for cities to evaluate and improve security. A maturity model is a set of structured levels that can describe the maturity of a process or complex system, and the degree to which it can reliably and sustainably produce required outcomes. There are generally five levels[26]:

1. *Initial* (chaotic, ad hoc, individual heroics) - the starting point for use of a new or undocumented repeat process.
2. *Repeatable* - the process is at least documented sufficiently such that repeating the same steps may be attempted.
3. *Defined* - the process is defined/confirmed as a standard business processes.
4. *Managed* - the process is quantitatively managed in accordance with agreed-upon metrics.
5. *Optimizing* - process management includes deliberate process optimization/improvement.

Public awareness campaigns, such as the recent attention over a security researcher's alleged attempts to infiltrate a plane's control systems that has served to draw attention to aviation security, can also be extremely helpful.

8. Conclusion

Successfully securing our cities would be a major step toward securing the nation from cyber attack. Unfortunately, significant obstacles stand in the way of realizing secure city-level infrastructures. By understanding a city's pressure points, and the interdependencies between critical and non-critical infrastructure sectors, we can test the limits of a municipality's defenses and find ways to mitigate vulnerabilities brought on by new technologies designed to improve energy efficiency and enhance livability. The Securing Smart Cities Initiative is a great first step in this process. By adding threat intelligence analysis to network operations centers, routinely conducting exercises and simulations, and initiating a robust penetration testing regime, any city can be a secure city.

[26] https://en.wikipedia.org/wiki/Capability_Maturity_Model