BUILDING THE SMART BASE OF THE FUTURE

The Integration of Smart Technologies for a More Efficent and Secure Base

Laura A. Nolan
Director, Cyber Programs and Exercises
National Strategic Research Institute (NSRI)
University of Nebraska
(410) 961-7914
lnolan@nsri.nebraskaresearch.gov

NATIONAL STRATEGIC RESEARCH INSTITUTE
at the University of Nebraska

INTRODUCTION

The world is experiencing a revolution in "smart" devices, intelligent and interconnected to improve our lives. Cities have been adopting smart technologies for years, almost out of necessity – it is near impossible to find new cameras, street lights, electronic signs, trains, or bridges that are not connected to an information network in some way. The evolution of technology continues to improve our way of life in many ways, such as adjusting supply to demand levels, identifying faults that require repair, tailoring information to the user, and gathering usage statistics to drive investments and improve services. This data, when analyzed, integrated, and leveraged to its full extent can improve not only the quality of life, but also economic growth, security, and safety for a city. The same is true for a military base, which is a city unto itself, and is also interdependent with its surrounding community. As these smart devices are connected to a network, the systems must be integrated to fully realize the potential value and must be secured from cyber threats to protect the data, people, and system itself. This paper proposes an approach to discuss smart bases and identify considerations for how to apply smart city concepts and methods to a military base.

The National Strategic Research Institute (NSRI) is a University Affiliated Research Center (UARC) and a trusted agent of the Department of Defense (DoD) affiliated with the University of Nebraska. NSRI presents this white paper in collaboration with Planet Defense, LLC to spur discussions about the progression toward smart bases and the necessary plans and considerations as we become "smarter."

WHY BUILD SMART BASES?

As a part of the larger national and global transformation, military bases are facing the same challenge as the communities within which these bases are located. Adding to this complexity are the major technological, economic, and environmental changes in the 21st century that are demanding appropriate transformational changes.

Cities and regions across the United States are increasingly engaged in social and economic transformation through smart city programs. Globally, we find similar trends. Military bases have the opportunity to use proven methods, technology, and principles from smart city implementation to design and build smart bases. Figure 1 depicts an effective smart base implementation that results in a secured intelligent infrastructure, energy-efficient buildings, efficient transportation, cost-effective operations, and higher quality of life for the inhabitants of the base.

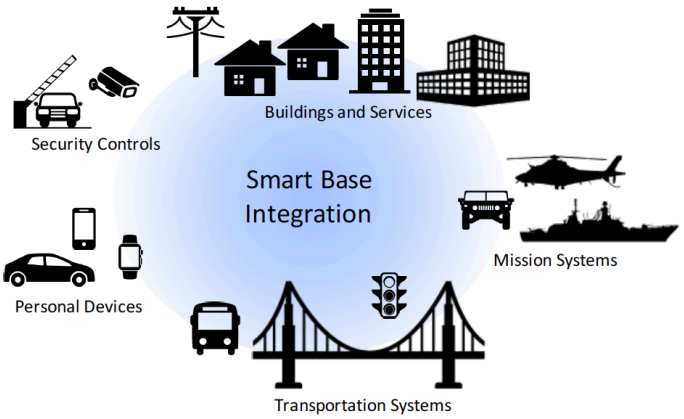

Figure 1: Smart Base Integration of Systems

Cybersecurity is increasing the security management challenge. Military bases can derive significant benefits by integrating cyber defense into smart base architecture. A similar approach has been advocated by Planet Defense, LLC for cities across America by integrating cyber defense and smart city programs. Since military bases are intertwined with local communities in many ways, the new smart city development presents an extraordinary opportunity for military bases to collaborate with the local community to overcome many of the shared challenges related to security, safety, disaster management, resource sharing, and national security.

WHAT IS A SMART BASE?

A military base is much like a self-contained city, with added security considerations. However, the base is not truly self-contained; it is interdependent with the surrounding community. The base is reliant on the critical infrastructure (e.g., power, gas, water, transportation) provided by commercial industry, just as any civilian city. The base provides many jobs and is often an economic driver for the surrounding area. A smart base is, therefore, just as critical to quality of life, economic growth, security and safety, and efficiency as a smart city.

The evolution of bases to become "smart" is inevitable. One driver is that as aging components require replacement, the commercial vendors are only offering "smart-enabled" devices. These devices are connected to computer networks regardless of whether or not that capability is leveraged. These connections are made through various technologies, namely Bluetooth, Wi-Fi, satellite, cellular, or hardwired. All new buildings, signs, cameras, etc. are connected to networks and smart-enabled by default. Base leadership must either disable all connections and change default passwords, or leverage the networked capabilities. Either path must be taken deliberately, otherwise the base systems are extremely vulnerable to cyber threats.

The remaining drivers of becoming a smart base are generally the same as the push toward smart cities.

- **Quality of Life**
  Local residents and workers of the base will experience improved satisfaction, innovation, and prosperity from better transportation and tailored services.

- **Economic Growth**
  As the base quality improves, the surrounding community that houses military and civilian staff will see increased economic growth of services, real estate, entertainment, construction, innovation, and contracting.

- **Security and Safety**
  Integrated physical security, information security, and personal safety monitoring increases overall security and safety for the people and systems on the base, including administration, logistics, financial management, and weapons systems.

- **Efficiency**
  Integrated monitoring, analysis, and control of connected systems create opportunities to improve investment and management decisions based on usage statistics, maintenance requirements, security, and safety.

A smart base can drive innovation and economic growth through synergy with DoD research initiatives. The DoD invests billions of dollars annually in research projects in many areas, including sensor grids, quantum computing, data analytics, artificial intelligence, and unmanned vehicles. This research requires large amounts of data and access to testing environments; the DoD invests heavily in generating this data, making it realistic enough for testing, and creating laboratory environments to conduct experiments. Smart bases present an opportunity to become a research testbed themselves and foster innovation. The smart base will possess a large amount and variety of data that can be used for a breadth of experiments. The data and operational systems should be protected from accidental or malicious modification, which is true for any operational system regardless if it's being used by researchers or not. This synergy of smart bases and research will improve efficiencies in investments and innovations for the future.

A few differences are apparent in the management of a smart base versus a smart city. A military base is more focused on security for access to secure facilities and weapons systems. A city is focused on public safety and privacy, where the people on a military base have inherently agreed to relinquish some privacy.

Privacy is lessened in exchange for access, security, and jobs when people show identification (which often requires social security numbers, background checks, and fingerprints) and allow their vehicle, bags, and person to be scanned and searched. In addition to the different balance between security and privacy, a city has a Mayor and government organizations responsible for different aspects of city management; while a military base is more regimented and orders can be given to create change. A city can create legislation and agreements, but they must work within the balance of power across the judicial, executive, and legislative branches of government. This balance of power is foundational to our civilian lives in the American public, but can also hinder integrated and timely sweeping changes. This military leadership of a base can be a benefit when integrating and securing smart technologies.

SMART BASE FRAMEWORK

The drivers of a smart base and its value proposition are clear; how to begin the implementation is less clear. We use the Smart Base Framework in Figure 2 to discuss the smart base and its components. These smart devices are known and proven technologies, with their integration being demonstrated in international smart cities. The evolution to a smart base can be implemented in phased approaches based on incremental funding, technology acceptance, or strategic initiatives.

The pillars of the Smart Base Framework are the components that comprise the interconnected system.

- **Security & Safety**
  Devices relevant to the security of the base's mission and the safety of the workforce include gates, badging access controls, traffic lights, electronic road signs, overhead street lights, and cameras.

- **Facilities & Infrastructure**
  The buildings on a base are frequently reliant on commercial power, gas, water, and network connectivity. Within a building, the elevators, escalators, lights, alarms, and heating, ventilation, and air conditioning (HVAC), are all part of the Building Automation System (BAS) network.

- **Personal Devices**
  The workforce uses government-provided equipment as well as personal equipment while on base. These systems will evolve toward the Internet of Things (IoT) and include laptops, phones, watches, cars, entertainment systems, toys, and health devices.

These smart-enabled components are all part of the smart base, whether the base leadership has direct control over them or not.

Across the top of Figure 2 is the integration of all these pillars together, which is where the base can realize gains and create opportunities. There is an increased uniformity in situational awareness for usage and anomalies that may not be apparent with localized visibility. Command and control of systems from a coordinated perspective creates efficiency through rapid prioritization and resource allocation. The management and collaboration of public/private partnerships is essential to smart base integration since the base is reliant upon and critical to its surrounding community.

This integrated system provides many benefits, but also introduces new cyber risks. Depicted as the foundation in the Smart Base Framework, a solid cyber security strategy and implementation is critical to a prosperous smart base. Potential adversaries include hacktivists, insiders, criminals, terrorists, and nation states and their motivations range from financial gain, to influence, to information dominance, to denial of service, to physical destruction. Examples of

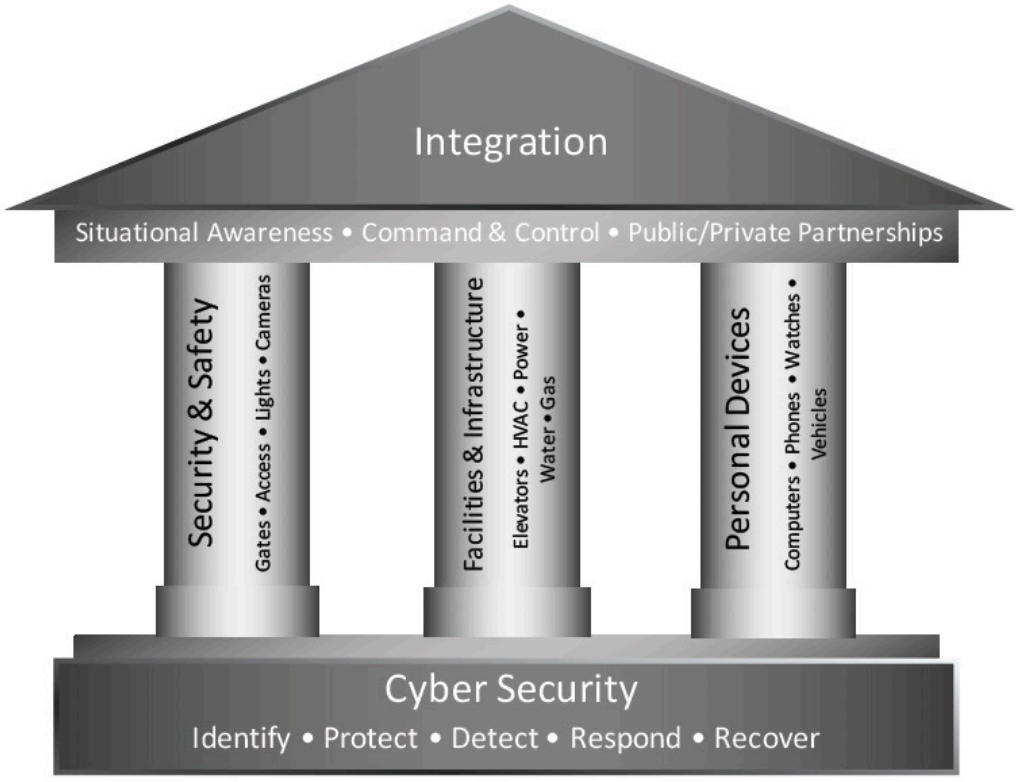

Figure 2: Smart Base Framework

attacks on critical infrastructure are becoming more and more prevalent. In December 2015 and 2016, electric power outages were caused in the Ukraine by the BlackEnergy malware and attributed to Russian actors. The outages lasted days in the dead of winter and, in 2016, caused long-term physical damage to some equipment[i]. In 2016, Mirai became a world-wide botnet of 300,000 IoT devices, such as cameras, TVs, switches, routers, DVRs, etc. The botnet spread rapidly and the attackers used the large collection of devices they now controlled in order to launch distributed denial of service (DDoS) attacks against popular websites, such as GitHub, Twitter, Netflix, Reddit, and Airbnb[ii]. The Trisis malware was found in a Saudi Arabian oil and gas refinery in August 2017. The malware operated with a misconfiguration which caused the industrial equipment to shut down, but
Trisis had the capability and intent to override physical safety mechanisms and cause physical destruction of the plant and its workers[iii]. In January 2018, SamSam ransomware encrypted Hancock Health's hospital email system, electronic health records, and internal operating systems. Despite having backup plans, the hospital paid the criminals $55,000 in ransom due to the time-critical, life-saving implications[iv].

These events demonstrate the sobering reality that threats are targeting our critical infrastructure and smart devices; we must prepare for these types of cyber attacks within our smart bases. The smart base design should utilize industry best practices[v] to architect the network and follow the National Institute of Science and Technology (NIST) Cybersecurity Framework[vi] to secure the network in a 24x7 operational environment. Industry best practices include network segmentation, multi-factor authentication, rolebased access controls, logical and physical security controls for critical components, and prompt deployment of security patches. The NIST framework for security operations includes the identification of all assets and key terrain, protection mechanisms (e.g., antivirus and firewalls), detection of suspicious events (e.g., anomalies and behaviors), response to stop or

minimize any negative effects, and recovery to a safe operational state. Due to the large scale of data in a smart base, machine learning, artificial intelligence, and visualization will be integral components in analyzing data at the speed of need and presenting information to decision-makers. As is becoming standard practice for cyber security across the critical infrastructure sectors[vii], collaboration and information sharing are key to rapidly understanding adversary tactics, getting ahead of the threats, and protecting the nation as a whole.

CONCLUSION

Technology evolution and the desire to improve quality of life, economic growth, security and safety, and efficiency are driving the U.S. military towards smart bases. The Smart Base Framework outlines the integration and cyber security considerations required during the implementation and operations of interconnected smart devices. In addition to benefits for the base community, the leadership of a smart base gain increased situational awareness, informed investment strategies, improved command and control, and alignment with DoD research innovation initiatives. The implementation of these concepts is not an all-or-nothing endeavor; the Smart Base Framework lends itself to phased adoption of known and proven technologies. The National Security Strategy 2018 calls for the United States to protect the "American way of life" and ensure American prosperity. International smart cities are already paving the way, and the DoD smart bases must lead the way for the U.S.

---

[i] How an Entire Nation Became Russia's Test Lab for Cyber War. https://www.wired.com/story/russian-hackersattack-ukraine/. Dec 2017.

[ii] Mirai: What You Need to Know About the Botnet Behind Recent Major DDoS Attacks. https://www.symantec.com/connect/blogs/mirai-what-you-need-know-about-botnet-behind-recent-major-ddosattacks. Sep 2016.

[iii] Trisis Has the Security World Spooked, Stumped and Searching for Answers. https://www.cyberscoop.com/trisisics-malware-saudi-arabia/. Jan 2018.

[iv] Ransomware Attack on Hancock Health Drives Providers to Pen and Paper. http://www.healthcareitnews.com/news/ransomware-attack-hancock-health-drives-providers-pen-and-paper. Jan 2018.

[v] Center for Internet Security. Top 20 Security Controls. https://www.cisecurity.org/controls/. 2018.

[vi] NIST Cybersecurity Framework. https://www.nist.gov/cyberframework. 2017.

[vii] Department of Homeland Security: Information Sharing. https://www.dhs.gov/topic/cybersecurity-informationsharing.