CYBER OPERATIONAL CONSIDERATIONS IN DENSE URBAN TERRAIN

Mad Science

Wed, 07/12/2017 - 4:02pm

Cyber Operational Considerations in Dense Urban Terrain

Paul Maxwell, Andrew Hall and Daniel Bennett

Introduction

Thirtieth Corps began its attack on the city of Metropolis and its 12 million inhabitants. The Corps planners had done their homework on urban operations and had studied many historical predecessors such as Stalingrad and Hue. Initially the attack proceeded well. Over time however, enemy indirect fire accuracy seemed to defy expectations given a lack of detected observers. Patrols were increasingly ambushed and leaders were targeted at an abnormal frequency. Raids failed to produce the desired results as targets were seldom found where they were expected. It seemed that the opponent knew their every move before they were executed. It soon became clear that the enemy had more capability than our intelligence sources briefed. The attack on the dense urban area stalled without success.

Scenarios like the one described are possible given our current training models and doctrine. Military operations are likely to occur in Dense Urban Terrain (DUT) similar to Metropolis due to demographic changes of modern society. DUT is a sub- set of Military Operations in Urban Terrain (MOUT) in which there is a corpus of knowledge. As described in the Army's Field Manual, FM 3-06, *Urban Operations*, the operational characteristics of this environment that the military should account for include physical, social, economic, and demographic factors. Many of these factors have been investigated and documented in the field manual and training products. Factors that have not been thoroughly discussed are the cyber characteristics of DUT and the impacts of those factors on military operations whether they are offensive, defensive, stability, or civil support. As the military analyses DUT and writes its doctrine on how to conduct operations and how to train in these environments, it is important to consider how cyber elements may influence the mission.

The urban areas in which military forces fight will certainly vary. They will range from low tech emerging cities to high tech smart cities. The structures, transport patterns, infrastructure, and footprints will be different. Despite these differences, they will possess a multitude of sensors connected by networks that can be leveraged for offensive or defensive purposes. Many of these sensors will be in the Internet of Things (IOT) devices that are exponentially growing in number. These devices can be connected together to provide useful functions to government officials, citizens, and military personnel [ZaB14]. Even the most technically limited cities are inundated with networked sensors in the form of mobile phones and the cyber operational potential of other cities only grows beyond that to varying degrees.

For the purposes of this work, the term cyber includes computer network operations and electronic warfare. Included in this analysis are the pervasive sensors, various network technologies, electro-magnetic spectrum issues, and the ability of modern artificial intelligence to analyse the digital mountains of data produced daily. Some of the threats and opportunities discussed currently exist and some are on the horizon and will become operational in five to ten years. Additionally, the conditions under which the operations are conducted will affect the impact of these systems. High intensity operations in DUT with evacuated populations will be less affected by some of these cyber considerations while low intensity operations will be more affected.

Technological Landscape of Dense Urban Terrain

Sensors

The rapid and cyclic advancement of technology has resulted in a proliferation of inexpensive yet capable sensors throughout the globe. These can have many forms and purposes. They can be commercially installed systems with a dedicated function to personally owned sensors that are general purpose in nature. Regardless of their intended use, they provide a rich palette of military options for those who wish to use them.

Cameras are everywhere, from the traditional surveillance cameras for security purposes to the ubiquitous cameras found in mobile devices and the growing population of unmanned aerial vehicles. There is little room for something to go unobserved by a camera in a city. It is estimated that there are close to a million cameras deployed in cities such as London and Beijing [ZhC15]. This does not even include cameras within homes that exist in computers, tablets, phones, smart televisions, security systems, etc.

Complementing the cameras are microphones. These sensors are frequently found in cell phones and other mobile devices. Increasingly, they are found in items such as surveillance cameras, toys, and even watches. Many of these devices are 'always on', such as the Amazon Alexa, listening for acoustic events and potentially recording all that they can sense to include nearby conversations.

Another common sensor is the accelerometer. These devices are capable of measuring movement in two and three dimensions. They are embedded in mobile devices to assist with navigation, orientation, and sometimes even for protection of the device in case they fall. Accelerometers are increasingly found in 'wearables' of all types too such as fitness trackers.

Magnetometers are in widespread use as well. These devices sense magnetic fields such as the earth's natural field or those resulting from the presence of ferrous objects. Typical applications include navigation (compasses) and counting/sensing objects such as vehicles. These devices are found in mobile devices, traffic management applications, and underneath our roadways.

Finally, there are numerous types of sensors connected to our urban infrastructure that measure things such as pressure in pipes, valve states (open/closed), temperatures, and volumes. These sensors are often connected to Supervisory Control and Data Acquisition (SCADA) devices to provide remote control over our water, electrical, and transportation infrastructure.

Networks

All of these sensors would be somewhat insignificant though were it not for the networks that connect them and allow them to share their data. The most well-known are the internet and cellular networks. DUT environments are often blanketed by both networks. Even emerging cities with poor internet penetration are frequently well covered by cellular networks. As discussed in the next section, even the network itself can be used as a sensor for use in military operations.

Other communications protocols can often be harnessed into Mobile Ad-hoc Networks (MANETs) or dedicated mesh networks thus allowing systems to share data. Technologies such as Bluetooth, Near-Field Communications (NFC), IEEE 802.15.4 (Zigbee), IPv6 Low-power wireless Personal Area Network (6LowPAN), and cognitive radios provide backbone capability to establish a sensor network.

With a network established, the power of these numerous sensors can be utilized. Whether it is through a deliberate design or surreptitious hacking of others' devices, the

(https://www.bakerinstitute.org/research/use-similarity-based-algorithms-predict-links-mexican-criminal-networks) by Rice University's Baker Institute for Public Policy

- Transnational Crime and Geopolitical Contestation along the Mekong (https://www.crisisgroup.org/asia/south-east-asia/myanmar/332-transnational-crime-and-geopolitical-contestation-mekong) by International Crisis Group
- China's Charm Offensive in Latin America and the Caribbean: A comprehensive Analysis of China's strategic Communication Strategy Across the Region [Part III: Image, Academia, and Technology] (https://digitalcommons.fiu.edu/jgi_research/57/) by FIU Digital Commons, Research Publications 57
- China's Charm Offensive in Latin America and the Caribbean: A Comprehensive Analysis of China's Strategic Communication Strategy Across the Region [Part II: Influencing the Media] (https://digitalcommons.fiu.edu/jgi_research/56/) by FIU Digital Commons, Research Publication 56
- China's Charm Offensive in Latin America and the Caribbean: A comprehensive Analysis of China's Strategic Communication Strategy Across the Region [Part I: Propaganda and Politics] (https://digitalcommons.fiu.edu/jgi_research/55/) by FIU Digital Commons, Research Publications 55
- Las bandas criminales de 3ª generación: un peligro para Chile (https://www.elmostrador.cl/noticias/2023/08/15/las-bandas-criminales-de-3a-generacion-un-peligro-para-chile/) by El Mostrador
- Amazon Underworld: Crime and Corruption in the Shadows of the World's Largest Rainforest (https://amazonunderworld.org) by Amazon Underworld
- Organised Crime as a Proxy: When Criminals meet Rogue States and Actors in Latin America (https://shoc.rusi.org/blog/organised-crime-as-a-proxy-when-criminals-meet-rogue-states-and-actors-in-latin-america/) by RUSI
- Mexico's 'Monster' Trucks Show Cartels Taking Drug War to Next Level (https://www.nytimes.com/2023/08/01/world/americas cartels-trucks.html?smid=tw-share) by New York Times
- Car Bomb Ambush injures at least Ten Guardia Nacional (GN) Agents in

data from these sensors can help a military force to accomplish its mission or contribute to its failure. The sensors and the connective tissue of the networks are continually present in DUT and therefore a factor that must be considered in the planning of urban operations.

Impact of Technology on Operations in Dense Urban Terrain

Maneuver and Intelligence

Tracking. In military operations of all types tracking friendly and enemy units is useful. Such information can assist with coordination, fire control, identification, and targeting. Traditionally, militaries accomplish this with methods such as networked gps devices, imagery, radars, and direction finding. In DUT environments, these methods may be limited or ineffective. However, cyber enabled devices can replace or supplement traditional methods.

An important feature of many of these cyber enabled sensors is their ability to track personnel and/or vehicles. Mobile devices, wifi, RFID, camera-based systems (e.g., vehicle plate recognition systems), and more support this type of intelligence gathering for those who wish to know [MiC13], [PaQ13]. This tracking can be low resolution tracking with only the ability to sense one or more objects or high resolution with the ability to identify and track specific targets. Tracking of this nature can be used for purposes such as intelligence gathering, targeting, and triggering fires. One could imagine using this type of tracking capability for applications such as geo-fencing [NaS13]. Geo-fences can establish areas that generate alerts when attacking forces enter them or when specific targets leave them.

An obvious tracking technology is based on video cameras. As previously discussed, cameras are everywhere in DUT environments. Whether it is securing a facility, providing public security, observing streets for traffic conditions, or taking selfies, the cameras are constantly capturing data. Deliberately configured or subsumed via cyber offensive operations, these video based systems such as the third generation surveillance systems in [Rat10] or the systems in [VaV05] and [BeR11] can detect, recognize, and track multiple objects. Their method for achieving this varies by system but all rely on distributed cameras, processing power (edge or centralized), and communications networks. Some systems [ZhC15] propose using under-utilized licensed frequencies such as UHF to communicate. Another system described in [AjB15] allows for users to query its surveillance database for events, generate alerts, and even predict future events. When connected to modern signal processing algorithms and artificial intelligence systems, this video data can provide valuable intelligence. This type of sensor network can allow for persistent identification and tracking of forces within the city. The ability to conceal operations or achieve tactical surprise may not exist in DUT environments.

Improved signal processing algorithms and cheaper processing power is enabling various tracking techniques based on electro-magnetic radiation. One such set of algorithms uses wifi for tracking movement. Research such as that done in [GoY15], [YaZ16], and [SoG16] demonstrate how wifi signals can be used to detect motion of human targets. Attributes of the wifi signals such as the Received Signal Strength, Time of Flight, phase of the signals, and channel state information are all used to detect movement. These systems have limited range and capability but given the widespread availability of wifi nodes in DUT environments, this technology could be adapted to provide early warning of opposing forces or indications movements by the populace. The work in [CoP14] used wifi signals as passive radar to detect and track moving vehicles at ranges up to 50m.

Other work in this area tracks targets but is more protocol agnostic and also supplements the inputs with other data types. The research in [SaW16] relies on a combination of signal analysis from wireless nodes and data from inertial measurement units (IMUs) or accelerometers. This system allows indoor navigation in what is usually a GPS denied region. Similarly, research using cell phones and the signals received from many sources (e.g., wifi, Bluetooth, 4G LTE, GPS, NFC) showed that large spaces could be radio frequency mapped in a crowd source technique thus allowing for navigation in GPS denied areas. Forces using this technology can navigate better inside the DUT environment where traditional navigation means are not as effective.

Data from devices connecting to wifi nodes can also provide a method for tracking individual devices. As shown in [AbB14], devices can be tracked passively by using data from connection logs in wifi access points. As devices interact with these access points, information about the device, such as it unique MAC address is logged. An ISR program could access these logs and use the data to track traffic flow in an area or even a particular device.

This type of tracking has also been shown to be feasible for Bluetooth devices. Using the information contained in these devices as they search to connect to other devices, movements of groups or individual devices can be mapped [StL11]. These low power sensors are common in many mobile devices and wearables thus creating a large population of data points.

Magnetometers provide another means of tracking targets. It is common for magnetic based systems to be embedded in roadways for traffic control. These sensors normally trigger traffic signals or count the number of vehicles passing a particular point to help transportation engineers improve traffic flows. If this data is shared via a wifi network then it is possible to track and with appropriate processing identify vehicles [KoO13]. Magnetic sensors may also be placed on the sides of roadways. The work of [WaZ15] showed how these sensors can count vehicles passing. This type of traffic flow data could help operations by identifying slow-go areas during intelligence preparation of the battlefield (IPB) or tracking convoy operations of opposing forces.

Due to a lack of line of sight (LOS) in DUT, radar systems would not frequently be incorporated into the Intelligence, Surveillance, and Reconnaissance (ISR) plan. Traditionally, these systems are employed in areas with clear LOS to allow their full tracking capability. FM 3-06 recommends only employing them on the peripheries of urban areas. However, enhancements in signal processing algorithms is making it possible for radars to work in Non-Line of Sight (NLOS) environments. [ZhZ16] showed how airborne radars (carried by heliostats) could track multiple targets in an urban environment using new processing algorithms. Additionally, dismounted personnel were tracked in a NLOS urban environment using X-band radars and new signal processing techniques. As computing power is improved and signal processing algorithms become more powerful, these systems will continue to break new ground.

Microphones when connected to additional processing power (Acoustic Processing Units) [HoN13] can detect acoustic events using the plethora of available sensors in DUT. These systems would detect an event (e.g., explosion, vehicle ignition), tag it with some metadata, and then forward it to a centralized server for additional processing. Devices such as these can monitor traffic density, approximate the number of people in a given space, and even identify and track specific vehicle types. Additionally, sound files from these devices have demonstrated the ability to identify which route a vehicle (or person) has travelled and in which direction [ScP13]. Even more simply, these devices can record the sounds around them to include voice communication and then forward those conversations to remote nodes for analysis. In this type of environment, every sound can be heard, recorded, and analysed.

Finally, cellular phones or other devices that connect to cellular networks provide a rich tracking capability. Each device provides an identifier to the cell nodes that it connects even if the device is not actively transmitting. This information is readily available in access logs for the cell nodes and can be used to track movements of the devices [BeC13], [RuS12]. This can help with targeting individuals. At a minimum, this technology should lead to a force protection consideration for those leaders who possess these devices.

Event Detection. Often it is desirable in military operations to detect when certain events occur. These events could be things such as perimeter violations, detection of a target in an area of interest, or the occurrence of detonations. On the current battlefield there already exists tools such as acoustic sniper detection/location devices and the unattended ground sensor. However, many of these were designed for and

transnational-organized-crime-threats-in-latin-america-converging-criminalized-markets-illicit-vectors/) by ICAIE (International Coalition Against Illicit Economies)

- Maximizing the potential of American irregular warfare in strategic competition (https://thehill.com/opinion/national-security/3928259-maximizing-the-potential-of-american-irregular-warfare-in-strategic-competition/) by The Hill
- Opinion: Don’t blur the lines by calling Mexican drug cartels ‘terrorist organizations’ (https://www.latimes.com/opinion/story/2023-03-17/dont-designate-mexican-drug-cartels-as-foreign-terrorist-organizations) by Los Angeles Times
- Armed Conflicts Spread Contaminated Water and Disease: Here’s How to Better Protect Civilians (https://www.justsecurity.org/85514/armed-conflicts-spread-contaminated-water-and-disease-heres-how-to-better-protect-civilians/) by Just Security
- Deterring the Next Invasion: Applying the Accumulation of Events Theory to Cyberspace (http://opiniojuris.org/2023/03/02/deterring-the-next-invasion-applying-the-accumulation-of-events-theory-to-cyberspace/) by Opinio Juris
- The next big threat to AI might already be lurking on the web (https://www.zdnet.com/article/the-next-big-threat-to-ai-might-already-be-lurking-on-the-web/) by ZDNET
- Migrant Caravans: A Deep Dive Into Mass Migration through Mexico and the Effects of Immigration Policy (https://www.bakerinstitute.org/research/migrant-caravans-deep-dive-mass-migration-through-mexico-and-effects-immigration-policy) by Rice University's Baker Institute for Public Policy
- Managing Risk for Special Operations Forces in Large-Scale Combat Operations (https://warontherocks.com/2023/02/managing-risk-for-special-operations-forces-in-large-scale-combat-operations/) by War on the Rocks
- The grey zone: Russia's military, mercenary and criminal engagement in Africa (https://globalinitiative.net/analysis/russia-in-africa/) by Global Initiative Against Transnational Organized Crime
- Deadly Rio de Janeiro: Armed Violence and the Civilian Burden (https://acleddata.com/2023/02/14/deadly-

work best in non-DUT environments where back- ground noise is limited and wave propagation models are simpler. The good news is that the density of networked sensors in DUT enables events of these types and more to be detected more easily than in other environments.

One scenario is to use the IMUs and compasses built into mobile devices to detect vehicle movement or even the occurrence of detonations (e.g., indirect fire, bombs, IEDs). [ReD13] showed that these sensors can detect and report the location and other data about earthquakes. With modified software, this could be extended to detecting large vehicle (e.g., tanks, IFVs) movement or other events that result in significant ground disturbance. A single or group of mobile devices could sense a passing vehicle through the vibrations their IMU detects and then forward that data to a central server with location and direction of travel.

Other work such as [KnP07] has demonstrated how blast events could be detected using microphones and signal processing algorithms. Once a microphone detects a blast, it adds location, time, and other metadata to an information file that is then sent to a server for further processing. Techniques such as this could be used to assist with determination of weapon accuracy and perhaps even allow for adjustment of indirect fires without an observer. Blasts could be pin-pointed to a location and compared against the target data to determine how to adjust subsequent rounds.

Movement. It is easy to envision how attacks (cyber or otherwise) on a city's infrastructure can impact the civilian populace and therefore hinder military operations. FM 3-06 discusses considerations for protecting or attacking these systems. However, not as well considered is how cyber enabled devices can also assist with military operations in DUT by influencing movement. Attacks on infrastructure control systems can augment movement by providing concealment. Additionally, they can detect or create congested movement corridors that have an effect on current operations. The bottom line is that a city's critical infrastructure must be considered during operational planning.

Critical infrastructure is often controlled via devices known as Supervisory Control and Data Acquisition (SCADA) devices. These systems provide remote, intelligent control over things such as our electrical grid, the water and gas distribution networks, and transportation systems. These systems exist in many places and with the development of the "smart city" concept, their numbers are sure to grow. As shown in the attack on the Ukraine's electrical grid, these systems can be vulnerable to cyber operations. A criminal, military, or other user with access can use these systems to the advantage of an operation. Deliberate use of these systems could provide counter-mobility effects or assist with the mobility of units for an operation.

As mentioned, the electrical grid contains SCADA devices. These devices can open and close switches to control power at the sub-station-level and below. In some cases, as discussed in [HiV11], this control can be narrowed down to a particular neighbourhood or block. Couple this with an increasing number of devices known as "demand response controllers" and you have the ability to target an increasingly narrow geographic area. This ability could allow an operator to turn-off power to areas of their choosing. This could help offensive operations by creating concealment through the elimination of electrical light sources or hurt a defensive operation by severing electronic-based C2.

Along these same lines is the water distribution network. This network consists of control stations containing networked sensors with SCADA controllers [UKY16]. These controllers are connected to valves that turn the water on and off. Similar to the electrical power scenario, an operator could use these SCADA controllers and sensors to deny water to select areas, create dangerous over-pressure areas, or even create mass leakages that undermine the above ground infrastructure.

Lastly, the transportation network's connectivity could be used to influence military movement. Traffic signals are increasingly monitored and controlled remotely. They also have increasingly powerful capabilities [Cisco][Surtrac]. The purpose is normally to alleviate traffic problems and provide data to assist with future traffic engineering.

rio-de-janeiro-armed-violence-and-the-civilian-burden/#s1) by ACLED

- North Korea's Political Warfare Strategy Has Failed: ROK – U.S. Alliance Needs A Superior Strategy (https://www.19fortyfive.com/2023/02/north-koreas-political-warfare-strategy-has-failed-rok-u-s-alliance-needs-a-superior-strategy/) by 1945
- Russia and Ukraine battle daily in the sky. So where are the pilots? (https://www.npr.org/2023/02/02/1153438336/russia-and-ukraine-battle-daily-in-the-sky-so-where-are-the-pilots) by NPR Morning Edition
- In Evaluating Immunities before a Special Tribunal for Aggression Against Ukraine, the Type of Tribunal Matters (https://www.justsecurity.org/84959/in-evaluating-immunities-before-a-special-tribunal-for-aggression-against-ukraine-the-type-of-tribunal-matters/) by Just Security
- China's Ferry Tale Taiwan Invasion Plan Is A Legal Nightmare (https://www.forbes.com/sites/jillgoldenziel/2023/01/3 ferry-tale-taiwan-invasion-is-a-legal-nightmare/?sh=ae43a885ceb1) by Forbes
- China Maritime Report No. 25: More Chinese Ferry Tales: China's Use of Civilian Shipping in Military Activities, 2021-2022 (https://digital-commons.usnwc.edu/cmsi-maritime-reports/25/) by CMSI China Maritime Reports.
- Hospital Ships: A Vital Asset for SOUTHCOM and South American Navies (https://cimsec.org/hospital-ships-a-vital-asset-for-southcom-and-south-american-navies/#comment-193434) by Center for International Maritime Security (CIMSEC)
- The Goshen Massacre and the Specter of Cartel Spillover Into the US (https://ioangrillo.substack.com/p/the-goshen-massacre-and-the-specter) by Narco Politics by Ioan Grillo
- Dangerous Alliances: Russia's Strategic Inroads in Latin America (https://ndupress.ndu.edu/Media/News/Article/325247 alliances-russias-strategic-inroads-in-latin-america/) by Strategic Perspectives 41, National Defense University
- Year Ahead – Emerging Technologies and the Collection of Battlefield Evidence (https://lieber.westpoint.edu/emerging-technologies-collection-battlefield-evidence/) by Articles of War, Lieber Institute

Instead, an operator could command these systems to cause congestion along a maneuver corridor or utilize the monitoring capabilities to understand movement patterns in the area as part of intelligence preparation of the battlefield.

Communications

Planning for military communications normally involves a variety of considerations (e.g., band allocations, emissions, line of sight) and covers technologies ranging from radio frequency to satellite to wired. This planning helps to ensure that friendly forces can communicate effectively and that we can detect, deny, and destroy enemy communications sources. However the combination of new technologies and the characteristics of DUT environments should force the consideration of other aspects.

Cognitive Radios. There is a growing research and commercial interest in cognitive radios. These devices use intelligent algorithms to sense the radio frequency environment for the purpose of providing reliable communications. These devices offer the possibility of creating communications networks using bands of frequencies that are currently restricted. The techniques vary but the general idea is that the radio communicates on empty/under-utilized frequencies and has the ability to cede the frequencies to higher priority devices upon detection of congestion. This means that a sensor network could be developed and emplaced that uses un-used television frequencies or FAA frequencies reserved for airports where none exist [JoN13].

This frequency flexibility can be useful not only in the commercial world to set- up inexpensive sensor and control networks without purchasing a license for a frequency band but also in the military domain. Frequency policies vary from nation to nation and thus production of devices and who can own them and transmit on them is controlled. The ability for the military to use radios that can alter the frequency range in which it operates could help decongest existing bands and improve communications [Elm13], [AkL06].

On the other hand, an adversary with this technology could create sensor or C2 networks in non-traditional bands thus making them hard to detect. Additionally, once identified, they technology is difficult to jam due to its sensing and intelligent channel switching. In the noisy RF environment of DUT, creating networks using this technology could make it difficult for military forces to find the enemy 'needle in a haystack' if you will.

Electro-magnetic Models. In the planning phases of operations, simulation tools are often used to plan communication node locations and to define the operational limits of the nodes for the forces involved. These tools rely upon signal propagation models to predict how well a signal will be received based on a selected location. Many of these models are line of sight (LOS) based and do not model well in areas with heavy NLOS sections and the related challenges faced due to multipath signals. Additionally, many of our military C2 systems rely upon adequate reception of signals to provide reliable data (e.g., GPS). Current systems do not reliably handle the NLOS DUT environment. Finally, the RF spectrum of DUT locations has not been well mapped for the vast array of urban environments that exist. What this spectrum looks like and how it will affect military communications is not well known.

There is a dearth of research on the effectiveness of military communications systems in DUT. How signals will propagate and the ability of systems to effectively communicate is not well characterized. One study has shown that the most common path-loss models do not accurately capture the realities of the environment [Xin15] from city to city. This is especially true in outdoor-to-indoor or indoor-to-indoor communications. Other work exploring low power transmitters such as those found in sensor networks describes the inadequacy of the models used for those devices [AlC16]. The authors propose the development of new algorithms and models to make better predictions on transmitter and receiver positioning. However, given the ever growing pervasiveness of emitting devices within an urban environment and the terrain that an urban environment presents to RF signals the ability to accurately model signal propagation, particularly deterministically, will be a fairly intractable problem for the foreseeable future.

- How Does 'Matter' Matter In International Conflict and Security? An Examination of the Importance of Mosques (http://opiniojuris.org/2023/01/12/how-does-matter-matter-in-international-conflict-and-security-an-examination-of-the-importance-of-mosques/) by Opinio Juris
- El Salvador Deploys Security Forces to Contain Criminal Groups (https://dialogo-americas.com/articles/el-salvador-deploys-security-forces-to-contain-criminal-groups/#.Y77pEC-B2X0) by Diálogo Américas
- Honduras declares war against gangs – and for control of popular narrative (https://www.theguardian.com/world/2023/jan/04/hond gangs-crackdown-xiomara-castro) by The Guardian
- Complexities and conveniences in the international drug trade: the involvement of Mexican criminal actors in the EU drug market (https://www.europol.europa.eu/publications-events/publications/complexities-and-conveniences-in-international-drug-trade-involvement-of-mexican-criminal-actors-in-eu-drug-market) by Europol-US DEA Analysis Report
- Mexico: Declassification of the Three Armed Conflicts Involving Drug Cartels on RULAC - The Geneva Academy of International Humanitarian Law and Human Rights (https://geneva-academy.ch/news/detail/587-mexico-declassification-of-the-three-armed-conflicts-involving-drug-cartels-on-rulac) by Geneva Academy of International Humanitarian Law and Human Rights
- Technology, Data, & The Future of Warfare: A Review Essay by James Torrence (https://digitalcommons.usf.edu/jss/vol15/iss4/9/) by Journal of Strategic Security
- Rinaldo Nazzaro, Leader of the Neo-Nazi Terrorist Group—The Base: Probable Linkages to the Russian Imperial Movement (RIM) (https://www.cofutures.net/post/rinaldo-nazzaro-leader-of-the-neo-nazi-terrorist-group-the-base-probable-linkages-to-rim) by C/O Futures Terrorism Research Note Series

DUT environments can be expected to have a very crowded RF spectrum. The number of transmitters is immense and includes things such as television, radio, wifi, cellular, Bluetooth, emergency services, airport and weather radars, and IOT devices. How all of these systems will impact military operations and systems is not well known. The authors of [AIT15] conducted a study to map the RF spectrum in an urban location. As expected, some bands are heavily occupied and thus jamming a system (e.g., cognitive radio network) in this region could impact many bystander systems. Additionally, they found there were many open bands in restricted ranges that could be utilized by intelligent cognitive radios. Much potential exists in the use of cognitive radios in that they can sense the environment in real time and then have the flexibility to react appropriately given that environment. However, given the uncertainty of knowing this environment ahead of time it can be very difficult to plan and coordinate the communications aspect of an operation in advance from a capacity and capability perspective.

Finally, the structures in many DUT locations create what are known as “urban canyons” where LOS dependent systems such as GPS receivers do not function well. Given the increasing reliance on GPS signals for navigation, C2, and precision weapon control access to these signals and the quality of the data therein is vital. As with many of the challenges mentioned, increasing computational power coupled with better algorithms can help. Work done by [WaG14] suggests that coupling 3-D models of DUT environments with signal processing algorithms can result in improved GPS location data in urban canyons.

Mesh and Other Networks. As previously discussed, DUT environments are flush with network devices. They are engineered to work on purpose-built networks for specific uses. Despite this, they are not limited to just that purpose. Ad-hoc mesh networks could be established either willingly or using malicious code to create C2 or sensor networks for an adversary. These networks can be dynamic and resilient in the face of changing device density and operational conditions.

One must also consider the use of designed networks for operational needs. There are numerous “apps” and other software on mobile devices that create communications platforms that can perform as C2 nodes. Some of these apps even provide end-to-end encryption capabilities that provide an unsophisticated opponent communications security on par with the most technologically advanced nations. The effectiveness of these non-traditional networks has been demonstrated in public movements such as the Arab Spring where masses of people were assembled and directed via social media and other applications. Military operations in DUT must consider how to monitor and when necessary utilize these means of communications to ensure operational success.

Conclusions and Future Work

Dense Urban Terrain presents numerous challenges and opportunities to military forces due its cyber characteristics. The volume of networked devices and communications platforms offers both offensive and defensive opportunities and challenges. The intelligence and command and control capabilities that these devices offer is unparalleled in other terrain. As discussed, these devices can impact maneuver, movement, and targeting as well. Without deliberate planning by operational staffs and appropriate action, it will be difficult to conceal operations and protect high value assets. It is necessary for the military to investigate these technologies more closely, to develop techniques for mitigating/utilizing them, and to create training environments where they can be used. Given the likelihood of conducting future operations in a DUT zone, it is imperative that we prepare adequately.

The preparation for this environment of course includes continuing work on the cyber security of our networks and critical infrastructure. Many of the issues discussed can be mitigated, or taken advantage of through thorough knowledge of their cyber security and electronic properties. Training should incorporate scenarios where IOT and mobile device sensors are used offensively or defensively to alter the operation’s outcome. Just as we learned to camouflage personnel and equipment to protect against visual detection and radars, troops need to learn how to camouflage operations from these networked sensors. Intelligence personnel need to learn about the data offered by these sensors and how to acquire that data. This can improve their IPB and their targeting. Electronic warfare units need to understand the evolving spectrum they face and the nature of the devices they will attempt to surveil or jam. Finally, continued research needs to be done to improve signal propagation models and signal processing algorithms so that planning tools and the use GPS devices within an urban environment can be improved.

The views of the authors are their own and do not reflect the views of the United States Military Academy, the United States Army, or the United States Government.

References

Abedi, N., Bhaskar, A., and Chung, E.,"Tracking spatio-temporal movement of human in terms of space utilization using Media-Access-Control address data", *Applied Geography*, Vol. 51, 2014., pp. 72 – 81.

Ajiboye, S. et. al., "Hierarchical video surveillance architecture: a chassis for video big data analytics and exploration" , *SPIE/IS&T Electronic Imaging*. International Society for Optics and Photonics, 2015, pp. 94070K1-94070K10

Akyildiz, I., et al., "NeXt generation/dynamic spectrum access/cognitive radio wireless networks: A survey", *Computer Networks*, Vol. 50, Iss. 13, 15 September 2006, pp. 2127 – 2159.

Alwajeeh, T., et al., "Efficient Method for Associating Radio Propagation Models with Spatial Partitioning for Smart City Applications", *ICC '16 Proceedings of the International Conference on Internet of things and Cloud Computing*, No. 8, Cambridge, United Kingdom, March 22 - 23, 2016, p. 7.

Al-Hourani, A., et al., "Spectrum occupancy measurements for different urban environments", *2015 European Conference on Networks and Communications (EuCNC)*, 29 June-2 July 2015, p. 6.

Bekhor, S., Cohen, Y., and Solomon, C., "Evaluating long-distance travel patterns in Israel by tracking cellular phone positions", *Journal of Advanced Transportation*, Vol. 47, 2013, pp. 435 – 446.

Benfold, B. and Reid, I., "Stable multi-target tracking in real-time surveillance video", *2011 IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, 20-25 June 2011, p. 8.

Bottero, M., Chiara, B., Deflorio, F., "Wireless Sensor Networks for Traffic Monitoring in a Logistic Centre", *Transportation Research Part C: Emerging Technologies*, Vol. 26, January 2013, pp. 99– 12.

Cisco, *Smart Traffic Management*, Available at: http://www.cisco.com/c/en_in/about/knowledge- (http://www.cisco.com/c/en_in/about/knowledge-network/smart-traffic.html) network/smart-traffic.html, (http://www.cisco.com/c/en_in/about/knowledge-network/smart-traffic.html) [Accessed 10 Nov 16].

Colone, F., et al., "WiFi-Based Passive ISAR for High-Resolution Cross-Range Profiling of Moving Targets", *IEEE Transactions on Geoscience and Remote Sensing*, Vol. 52, Iss. 6, June 2014, pp. 3486 – 3501.

Elmasry, G., "The Progress of Tactical Radios from Legacy Systems to Cognitive Radios", *IEEE Communications Magazine*, Oct 13, pp 50 – 56.

Gong, L., et al., "Wifi-based Real-time Calibration-free Passive Human Motion Detection", *Sensors*, Vol. 15, 21 December 2015, pp. 32213 – 32229.

Gustafsson, M., et al., "Extraction of Human Micro-Doppler Signature in an Urban Environment Using a "Sensing-Behind-the-Corner" Radar", *IEEE Geoscience And Remote Sensing Letters*, Vol. 13, No. 2, February 2016, pp. 187 – 191.

Higgins, N., et al., “Distributed Power System Automation With IEC 61850, IEC 61499, and Intelligent Control”, *IEEE Transactions On Systems, Man, And Cybernetics—Part C: Applications And Reviews*, Vol. 41, No. 1, January 2011, pp. 81 – 92.

Hollosi, D., et al., “Enhancing Wireless Sensor Networks with Acoustic Sensing Technology: Use Cases, Applications & Experiments”, *2013 IEEE International Conference on Green Computing and Communications (GreenCom), and IEEE Internet of Things and IEEE Cyber, Physical and Social Computing (iThings/CPSCom),* 20-23 Aug. 2013, pp. 335 – 342.

Joshi, G., Nam, S., and Kim, S., “Cognitive Radio Wireless Sensor Networks: Applications, Challenges and Research Trends”, *Sensors*, Vol. 13, No. 9, 2013, pp. 11196 – 11228.

Knobler, R., and Plummer, T., “Time Difference of Arrival Blast Localization Using a Network of Disposable Sensors”, *Sensors, and Command, Control, Communications, and Intelligence (C3I) Technologies for Homeland Security and Homeland Defense VI*, ed. Edward M. Carapezza, Vol. 6538, 2007, p. 11.

Kostakos, V., Ojala, T., and Juntunen, T., “Traffic in the Smart City: Exploring City-Wide Sensing for Traffic Control Center Augmentation”, *IEEE Internet Computing*, Vol. 17, Iss. 6, Nov.-Dec. 2013, pp. 22 – 29.

Michael, K, and Clarke, R., “Location and Tracking of Mobile Devices: Uberveillance Stalks the Streets”, *Computer Law & Security Review*, Vol. 29, 2013, pp. 216 – 228.

Mirowski, P., et al., “SignalSLAM: Simultaneous localization and mapping with mixed WiFi, Bluetooth, LTE and magnetic signals”, *2013 International Conference on Indoor Positioning and Indoor Navigation (IPIN),* 28-31 Oct. 2013, p. 10.

Namiot, D., and Sneps-Sneppe, M., “Geofence and Network Proximity”, *Internet of Things, Smart Spaces, and Next Generation Networking*. Springer, Berlin Heidelberg, 2013, pp. 117 – 127.

Pan, Gang, et al. "Trace Analysis and Mining for Smart Cities: Issues, Methods, and Applications,"

IEEE Communications Magazine, Vol. 51, No. 6, 2013, pp. 120 – 126.

Raty, T., “Survey on Contemporary Remote Surveillance Systems for Public Safety”, *IEEE* (http://ieeexplore.ieee.org/xpl/RecentIssue.jsp?punumber=5326) *Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews)* (http://ieeexplore.ieee.org/xpl/RecentIssue.jsp?punumber=5326), Vol. 40, Iss. 5, (http://ieeexplore.ieee.org/xpl/tocresult.jsp?isnumber=5550332) September 2010, pp. 493 – 515.

Reilly, J., et al., “Mobile Phones as Seismologic Sensors: Automating Data Extraction for the iShake System”, *IEEE Transactions on Automation Science and Engineering*, Vol. 10, Iss. 2, April 2013, pp. 242 – 251.

Rubio, A., Sanchez, A., and Frias-Martinez, E., “Adaptive Non-parametric Identification of Dense Areas Using Cell Phone Records for Urban Analysis”, *Engineering Applications of Artificial Intelligence*, Vol. 26, Iss. 1, January 2013, pp. 551 – 563.

Savic, V., Wymeersch, H., and Larsson, E., “Target Tracking in Confined Environments with Uncertain Sensor Positions”, *IEEE Transactions on Vehicular Technology*, Vol. 65, Iss. 2, February 2016, pp. 870 – 882.

Schuller, B., et al., “Acoustic Geo-Sensing: Recognising Cyclists' Route, Route Direction, and Route Progress from Cell-Phone Audio”, *2013 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP),* 26-31 May 2013, p. 5.

Soldovieri, F., and Gennarelli, G., “Exploitation of Ubiquitous Wi-Fi Devices as Building Blocks for Improvised Motion Detection Systems”, *Sensors*, Vol. 16, No. 307, 27 February 2016, p. 13.

Stange, H., et al., “Analytical Workflow of Monitoring Human Mobility in Big Event Settings using Bluetooth”, *ISA '11 Proceedings of the 3rd ACM SIGSPATIAL International Workshop on Indoor Spatial Awareness*, Chicago, IL, 1 November 2011, pp. 51 – 58.

Surtrac, “Smart Traffic light”, Available at: https://www.surtrac.net/, (https://www.surtrac.net/) [Accessed 8 November 2016]. University of Kentucky, “Water Distribution System Toolkit”, Available at: http://www.uky.edu/WDST/SCADA.html, (http://www.uky.edu/WDST/SCADA.html) [Accessed on 2 November 2016].

Valera, M., and Velastin, S.A., “Intelligent Distributed Surveillance Systems: a Review”, *IEE Proceedings - Vision, Image and Signal Processing*, Vol. 152, Iss. 2, 8 April 2005, pp. 192 – 204.

Wang, L., Groves, P., and Ziebart, M., “Smartphone Shadow Matching for Better Cross-street GNSS Positioning in Urban Environments”, *The Journal of Navigation*, Vol. 68, 2015, pp. 411 – 433.

Wang, Q., et al., “Analysis and Experiments of Vehicle Detection with Magnetic Sensors in Urban Environments”, *2015 IEEE International Conference on Cyber Technology in Automation, Control, and Intelligent Systems (CYBER),* Shenyang, China, 8-12 June 2015, pp. 71 – 75.

Qian, Xing. “*Peer-to-peer Urban Channel Characterization for Military UHF Band*,” Diss. 2015, p. 137.

Yahui, W., and Xiaoran, G., “The Study of Location Technology Based on Wireless Sensor Networks in Smart City”, *2016 12th IEEE International Conference on Control and Automation (ICCA),* Kathmandu, Nepal, 1-3 June 2016, pp. 848 – 853.

Zanella, A., et al., “Internet of Things for Smart Cities”, *IEEE Internet of Things Journal*, Vol. 1, Iss. 1, February 2014, pp. 22 – 32.

Zhang, T., et al., “The Design and Implementation of a Wireless Video Surveillance System”, *Proceedings of the 21st Annual International Conference on Mobile Computing and Networking*, pp. 426 – 438.

Zhou, M., Zhang, J., and Papandreou-Suppappola, A., “Multiple Target Tracking in Urban Environments”, *IEEE Transactions on Signal Processing*, Vol. 64, Iss. 5, March 1, 2016, pp. 1270 - 1279.

Categories: urban operations (/taxonomy/term/495) - sensor networks (/taxonomy/term/503) - Mad Scientist (/taxonomy/term/306) - electronic warfare (/taxonomy/term/504) - dense urban terrain (/taxonomy/term/505) - cyber operations (/taxonomy/term/379)

About the Author(s)

Paul Maxwell (/author/paul-maxwell)

Dr. Paul Maxwell is the Cyber Fellow of Computer Engineering at the Army Cyber Institute and an Associate Professor in the department of Electrical Engineering and Computer Science at West Point. He served 24 years in the Army as an Armor officer. His military assignments include Battalion Executive/Operations Officer, Brigade Logistics Officer, Company Commander, Scout Platoon Leader, Company Executive Officer, and Mechanized Infantry Platoon Leader. He is a

member of the Institute of Electrical and Electronics Engineers (IEEE) and is a CISSP. His research interests include programmable logic, computer architecture, robotics, robustness, and cyber policy.

Andrew Hall (/author/andrew-hall)

Colonel Andrew O. Hall was commissioned in 1991 from


(/author/andrew-hall)

Colonel Andrew O. Hall was commissioned in 1994 from the United States Military Academy as an Infantry Officer. He has a BS in Computer Science, a MS in Applied Mathematics, and a Ph.D. in Management Science. He previously served as the Chief of the Military Personnel Structure and Plans Division in the Army G-1 where he was instrumental in the establishment of the Cyber Branch and is currently assigned as the Director of the Army Cyber Institute at West Point.


(/author/daniel-bennett)

Daniel Bennett (/author/daniel-bennett)

Colonel Dan Bennett was commissioned a distinguished military graduate in 1994 from the Colorado School of Mines as a Signal Officer. He has a B.S. in Engineering (Electrical Specialty), and an M.S. and Ph.D. in Electrical Engineering. His most recent operational experience was as the Cyberspace Operations Infrastructure and Special Projects lead for the Commander of the Cyber National Mission Force, U.S. Cyber Command. He is currently assigned as the Chief of Research of the Army Cyber Institute at West Point.