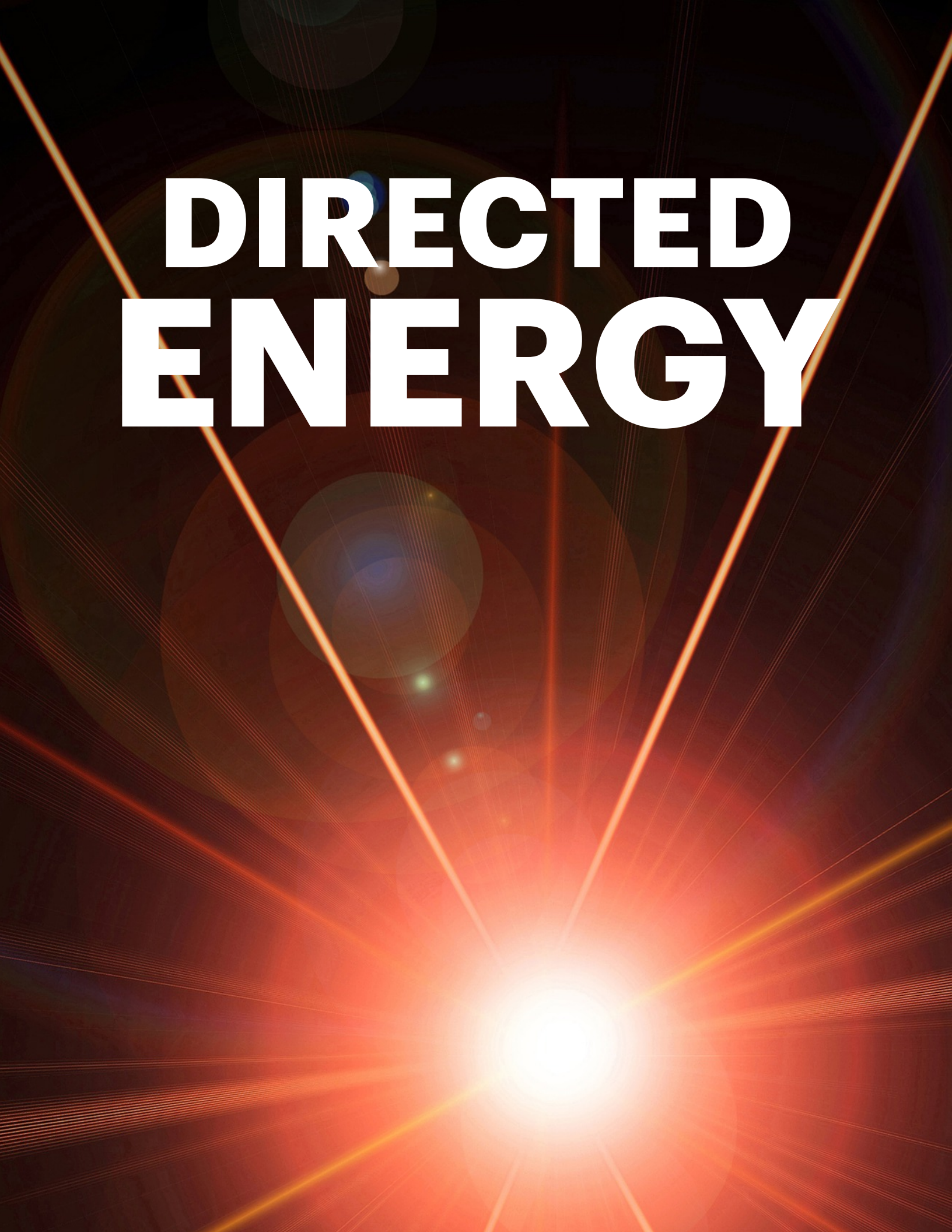

11TH ANNUAL
HOMELAND
SECURITY WEEK
3 CRITICAL FACETS TO
SECURING THE
HOMELAND
eBook
www.homelandsecurityweek.com
1-800-882-8684 ● enquiry@iqpc.com

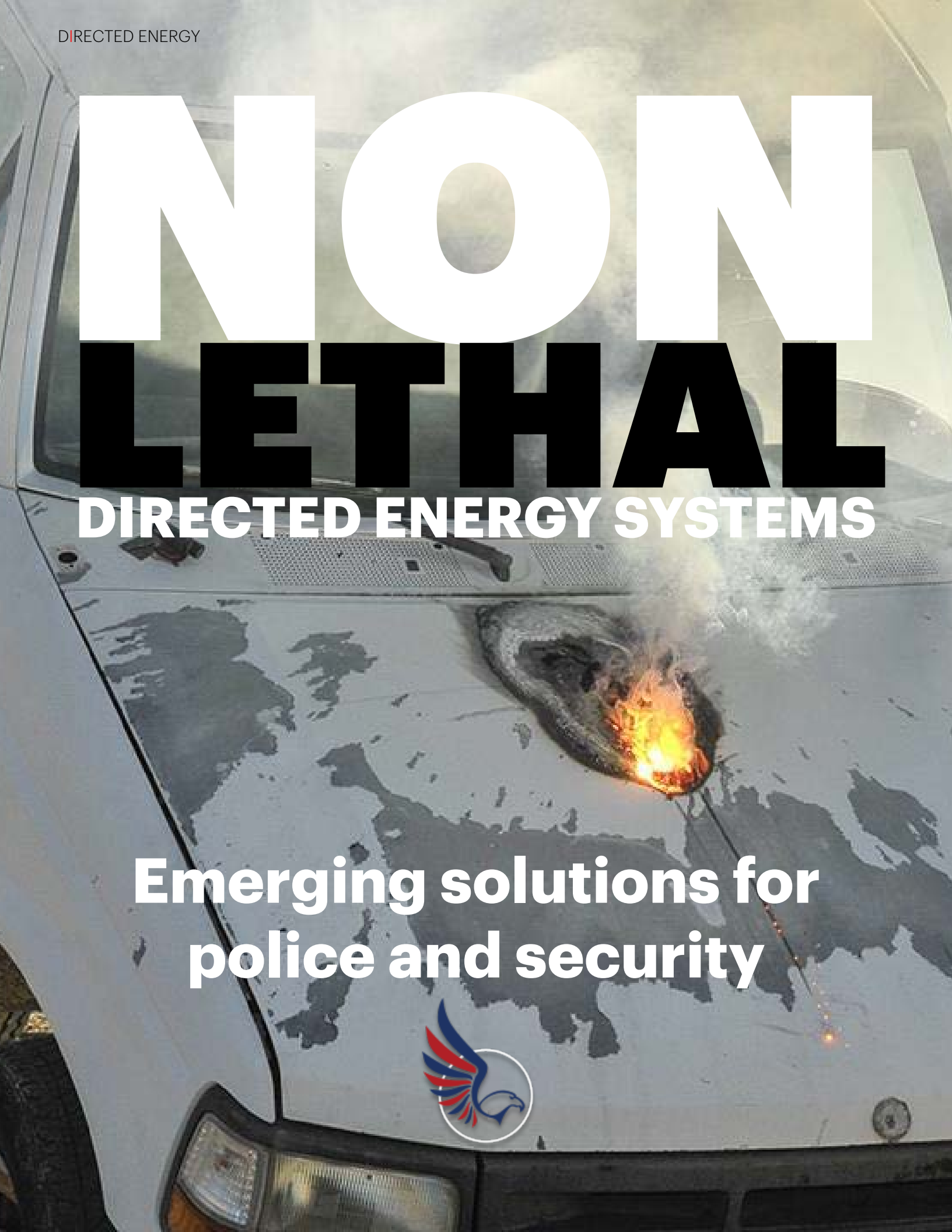
November 1 – 3
Washington D.C.

11TH ANNUAL HOMELAND SECURITY WEEK

Ensuring homeland security is a moving target—an on-going and eternally evolving battle. The latest technological changes, as well as the socio-political environment, both at home and abroad, contribute to the difficulty of the task.

In advance of **Homeland Security Week**, we've made it our mission to inform you of the latest innovations to facilitate the maintenance of a current and complete big picture view, so that you can more effectively do your duty.

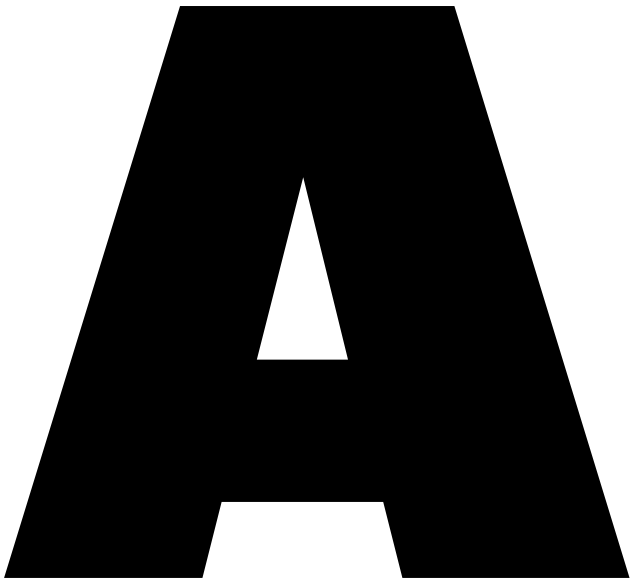

DIRECTED
ENERGY



NON LETHAL

DIRECTED ENERGY SYSTEMS

Emerging solutions for police and security



longside recent studies assessing the global police and law enforcement equipment market set to grow at a CAGR of 3.98% over the period 2014-2019, non-lethal (or less than lethal) weapons are currently experiencing a growth in demand among law enforcement agencies worldwide.

Further market figures indicate that this trend is expected to continue, and for a number of reasons. For one, the ongoing spread of democracy, of freedoms and of mass communication – all in themselves positive – inevitably allow for greater opportunity to protest or revolt against the authorities. Most democratic governments recognise the need to not only allow peaceful protest but to curb violent disorder with non-violent measures, avoiding the risk of harming civilians or inciting further violence.

Meanwhile, the global risk of urban dissent, terrorism and insurgency has been steadily on the rise, requiring a police response that is as rapid as it is even-handed to the situation. Investment into the research, development, and procurement of non-lethal weapons has recently included crowd control systems such as tear gases, malodorants, water cannons, sticky foam and electroshock solutions – all with varying degrees of success. However, directed energy represents a range of fledgling technology, some of which may well prove to be game-changers for the future of law enforcement.

Engine-stopping

At the beginning of 2015, Lockheed Martin successfully completed a test of its new directed energy system that saw it stop a truck from over a mile away. Known as ATHENA (Advanced Test High Energy Asset), the technology was able to place a 30 kW fibre-optic laser on the vehicle, burn quickly through the body and destroy the engine at a range of 1.6 kilometres.

The system is based on the company's earlier Area Defense Anti-Munitions (ADAM) programme, an experimental short range ground-to-air anti-missile weapons system that employed multiple 10 kW fibre lasers. ADAM conducted successful tests against military-grade small boats in 2014 – disabling them in under 30 seconds at a distance of 1.6 km – and remains in prototype phase. However, the company believes the single (or combined) 30 kW beam provides "greater efficiency and lethality".

In the ATHENA test, the truck was not driving but instead towed on a platform with its engine and drivetrain running. There are naturally further tests to be undertaken at increasingly difficult thresholds, but current progress already marks a milestone not only for Lockheed Martin but the wider field of DE systems in the military space.

The capability of safely shutting down vehicles at a distance remains a desirable goal for both military, security and law enforcement, whether the threat is terrorist or high-end military. However, with discussions continuing over

reliability, safety and budgets, the rate at which these will be adopted in active service remains in question.

“Any object or individual in the line of sight of a high energy laser beam, even if very far from the intended target, is in severe danger,” says Rear Admiral (Rtd) Massimo Annati, Chairman of the European Working Group on Non-Lethal Weapons. “But EMP is a little more complex. Engine stoppers, or systems used to counter RC-IEDs are already operational and fielded. As a destroyer-inhibitor of electronic components in communication networks and computers, there are still some obstacles to overcome and, despite some new announcements, a fieldable and reliable solution is not expected for tomorrow.”

Anti-riot systems

Other solutions in this space that have been under consideration and development include more controversial solutions, such as Raytheon’s Active Denial System (ADS), a vehicle-mounted system designed to heat the skin of a human target for us in area denial, perimeter security and crowd control. That concept involved subduing the person with an intense but temporary pain that has no lasting physical effects.

The US military deployed ADS to Afghanistan in 2010 but it was ultimately withdrawn without seeing combat. A version is currently being tested in a six-month pilot scheme by the LA County Sheriff's Technology Exploration Program, under the name ‘Assault Intervention Device’. Here, the system will attempt to breakup fights or riots by providing a momentary ray of heat on a combative individual to distract them or cause them to move away from an area, thereby allowing a short window of time for correctional officers to take control of the situation. US Marines and police officers are also exploring man-portable versions.

Most nations in the West will of course face some of the most rigid legal requirements to ensure safe and responsible design and application, and will of course have a particularly difficult challenge in winning public acceptance. Other parts of the world undoubtedly have fewer barriers to development and deployment.

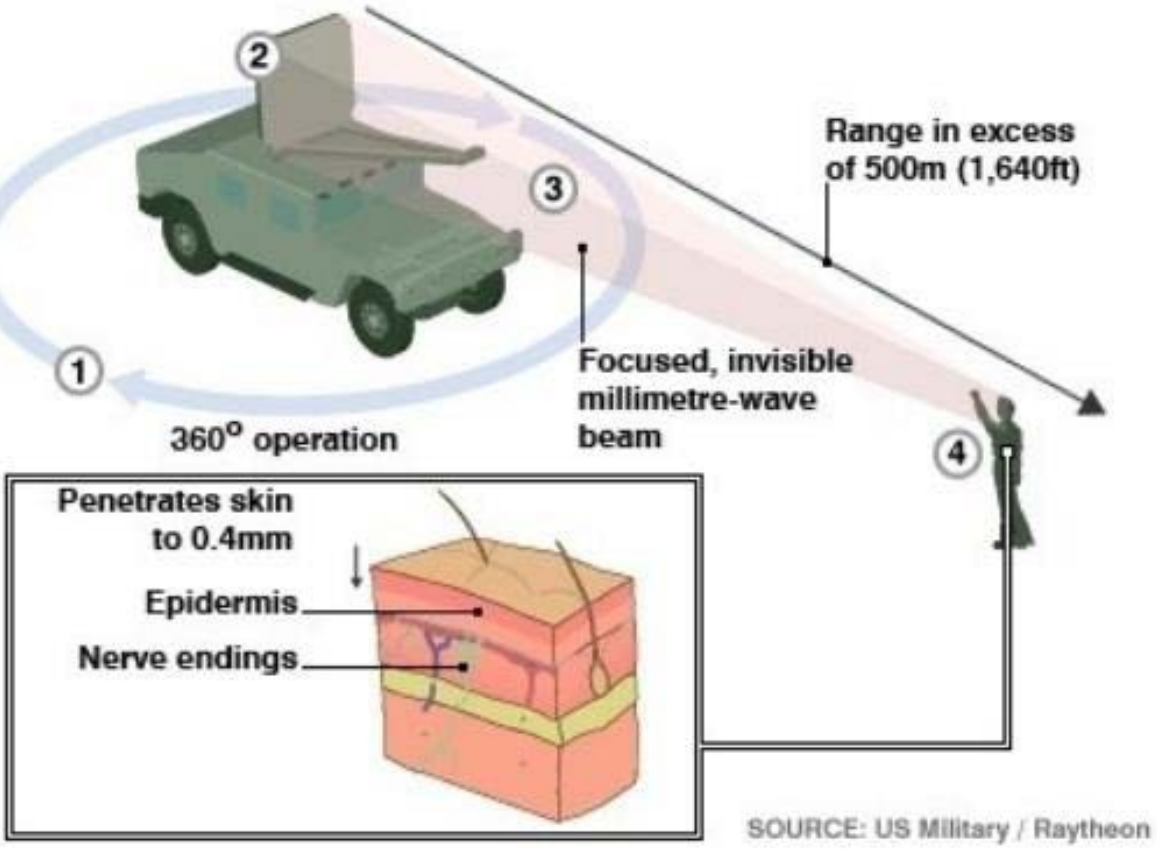
The China Poly Group Corporation has unveiled the development of its WB-1 millimeter-wave beam-projecting non-lethal anti-riot system, which heats molecules beneath the human skin. The system is said to have an effective range of between 80 m to 1 km.

Russia has also revealed that it is working on a similar weapon that implements high-frequency radiation to cause intolerable heat on the skin within seconds. That device – understood to be a smaller, lower-powered version of its US counterparts – is said to have a range of about 300 yards.

Outlook

The adoption of new directed energy technology is an exciting prospect, but it also comes with serious concerns regarding obsolescence. Regulations are likely to change and adapt as new research is undertaken and operational experience either highlights or disproves safety concerns on a case-by-case basis.

If proven both safe and effective, the next consideration will be long-term affordability. While directed energy is touted as a cheaper alternative to many other options, such as water cannon or gas grenades, any system needs to prove that it can offer low costs when it comes to powering, integration on vehicles, and maintenance, while also meeting clear-cut capability needs such as fast rate of regeneration and ease of mobility.



The Navy is experimenting with lasers... we explored their findings.

VIEW THE FULL PIECE

WATCH THE VIDEO

BIOMETRICS

James A. Loudermilk is the Senior Level Technologist for the FBI Science and Technology Branch. James focuses upon identification issues, especially biometrics, and frequently represents the FBI on these topics. Recently he served as the Department of Justice co-chair of the Biometrics and Identity Management Subcommittee of the National Science and Technology Council.

WHAT WE NEED TO DO THE JOB

What are some key challenges in the area of biometrics that you are facing at the Department of Justice?

Our longest operating program – fingerprints – has achieved unprecedented search reliability at 99.6% TAR with a 0.1% FRR. Which is wonderful. However, our daily volume averages more than 145,000 tenprint checks a day, 365 days per year. With that volume of activity there remain a lot of potential misses. And some misses can have serious consequences. We need to improve the image quality of the underlying fingerprint data in the criminal master file. Commercial surveillance cameras have proliferated and increasingly criminal activity is captures on video and slow scan systems. Again, image quality is an issue. Face matching performance has dramatically improved over the past two decades, yet still often produces an excessive volume of leads referred to human analysts. The ability to effect cross-spectral matching between low light and infrared surveillance imagery and conventional visible light arrest mugshots falls well short of desired performance.

The FBI is seeking vendors for a mobile biometrics app, can you tell us who they are considering for this application, and how exactly you see this app being implemented in the field?

No. Procurement related activity is extremely sensitive. But what I can tell you is that the Next Generation Identification program introduced a fingerprint Repository of Individuals of Special Concern (RISC) and mobile fingerprint "stoplight" matching has been deployed as a national service. We have had well over a million searches (*searches only, enrollment must be done subsequent to arrest at the booking station*) with about a 7% "hit" rate. This tool can greatly reduce officer workload as well as reduce the number of arrests in ambiguous identity situations. Approaching half the states are participating in this program although as yet relatively few officers have been issued mobile fingerprinting equipment.

> "The technology is showing great progress and the necessary infrastructure changes have been identified."

What are you most excited about in the area of biometrics technology, and are you personally involved in any new projects for solving identification issues?

Both personally and organizationally we are very excited about the prospects of introducing rapid DNA collection and analysis into the booking environment with its potential of linking arrestees to serious violent crimes while the suspect is still in custody. The technology is showing great progress and the necessary infrastructure changes have been identified. However, as Director Comey recently noted during testimony it does require legislation before the technology can be used outside accredited DNA laboratories. Video analytics offers great promise and we are seeing significant progress.

Mr. Lee Bowes currently is assisting U.S. Citizenship and Immigration Services (USCIS) in developing strategies that focus on more person-centric aspects of identity management and data usage. Below he gives his perspective on the biometrics division, which over just this year collected biometrics on 3.8million individuals across 138 domestic sites and many international locations.

PERSON-CENTRIC BIOMETRICS

Can you explain your assistance with the USCIS in developing a more person-centric focused strategy, how have you gone about this, and what are its benefits?

The majority of my work with biometrics in USCIS has been operational in nature. We collect over 3 million new sets of biometrics every year, and my role has been ensuring that this information is collected, used, and stored correctly. Being in-tune with the daily operations, and being responsible for correcting any problems that arise, has given me insight into the areas where improvement is needed.

Treating biometrics as person-centric information, rather than transactional information, is really not overly difficult to explain. The key is to get people to think of treating data as it exists in the real physical world, and not as it exists in IT systems.

The efforts I've been leading have focused on developing systems and processes around the "real world" concept. The largest part about advocating and leading these changes is educating the various stakeholders of the status quo. Moving toward person-centric processing requires a large amount of up-front work to address the legal and policy implications of changing the current business process. Many users and decision-makers have only a thinly-sliced view of the whole biometric picture, but once the larger realm of biometrics systems and capabilities is disseminated, the benefits become quite apparent.

For USCIS, the benefits are multiple. Person-centric processing hinges on the concept of establishing an identity at the beginning of the immigration lifecycle, and utilizing that same identity through the remainder of interactions. This includes identity verification with each encounter with an immigration applicant, which reduces or eliminates imposter fraud risk to both USCIS and the applicant. Verification is also more efficient than (re)collection, which benefits both USCIS and the applicant in terms of time and money."

The FBI has said it is looking for a phone application capable of mobile biometrics, how do you see this improving the process, and where would it be used the most?

For USCIS, I see mobile biometrics as a substantial benefit to the application process. USCIS Transformation is adding the capability for applicants to create an online account from which they can submit applications and maintain personal information. While electronic authentication and identity-proofing is quite effective in managing an online identity, there is a "gap" that occurs between online identity creation and the physical, biometric identity establishment. Mobile biometric collection could assist in tying biometrics to online events, which could then serve to verify the same identity acting online as the identity appearing in USCIS offices.

"One form of mitigation to dissemination issues is cross-component access to various systems."

What are some key challenges facing the Biometrics Division in the USCIS ?

One challenge is bringing great ideas and new capabilities into operation quickly. While we may be able to quickly solve technical challenges, each change has to be examined to determine impact on regulation, policy, privacy, and legacy operations.

From a data and identity management perspective, we face a challenge in relating non-biometric events (document issuance, appointments, name-based background checks, etc) with biometric identities. While account numbers and the like are (in theory) singular to a person, they are easily mistyped.

Many other biographic identifiers change or are provided differently (hyphenated names, middle initials, address units), making comprehensive identity management difficult to implement in the midst of legacy systems and data.

What do you believe can be done to improve the process of collection, storage, and dissemination of biometric data, that isn't being done?

I think collection and storage is done quite well in USCIS and DHS in general, but we have much room for improvement in dissemination and access. Dissemination of biometric data is relatively streamlined for components utilizing the DHS-IDENT database; however, contextual data surrounding the biometric identity is a different story. Part of this reason is that contextual data (for example: immigration status, privacy flags, travel information) largely resides in legacy systems hosted by the responsible component. These legacy systems are not designed to interface in the real-time, service-oriented architecture that new systems are built upon. This means interfaces are stove-piped, or worse, rely on manual data uploads – which results in data latency and integrity issues.

One form of mitigation to dissemination issues is cross-component access to various systems. However, this too is a challenge given the multitude of authentication mechanisms (mainframe, database, active directory, ICAM). Without a more central or shared management of system access, DHS employees will be scattered across varying levels of systems access, which causes discrepancies in data knowledge."

SUMMIT SESSION

Biometric Requirements to Protect Critical Infrastructure

November 3 - 1330

THE FUTURE OF FACIAL RECOGNITION

In this interview, **Dr. Thirimachos Bourlai**, an expert at the forefront of face recognition technology, shares his opinions on what the federal government stands to learn from private industry developments in facial recognition technology. He also sheds light on quality metrics for practical facial recognition and details some the up-and-coming technology that will be used in the future to deal with problems of recognizing unfamiliar faces and research in video biometrics.

What can the federal government learn from private industry developments in terms of facial recognition technology? What are the challenges in face recognition?

One of the physiological traits utilized by biometric systems to establish human identity is face. Face-based recognition systems are gaining increasing interest, especially over the last decade, because the human face has several advantages over other biometric traits. It is non-intrusive, understandable, and can be captured in a nonintrusive manner at variable standoff distances and using variable camera sensors.

A typical face recognition system consists of two main phases, i.e. the enrollment and the authentication phase.

During the enrollment phase, images of the users' face are taken and used to create face templates that are stored in a database, typically called the gallery dataset.

During the authentication phase, newly recorded images of a user's face, called probes, are used for recognition. A decision on the person's identity (the output of a FR system) is taken on the basis of the comparison between the gallery templates and the new (probe) images. In simple words, the similarity between two face images of the same person that is delivered by a face recognition system is expected to be higher than the similarity between face images of different individuals.

The question is whether this is always true when operating in real-world conditions. Unfortunately, in practice, things are not that straight forward. There are various challenges with regards to facial recognition technologies and that is why there are so many groups worldwide that work in this area. I would narrow the challenges down into four main categories:

1) **Person-related:** variations in pose, expression, illumination etc.

2) **Device-related**: using different camera sensors such as (i) cameras operating at different spectra, (ii) very expensive, high-end vs. low cost surveillance cameras, (iii) cameras on mobile platforms such as cellphones or tablets etc.

3) **Related to FR matching software used:** (i) commercial software packages in which the operator cannot access, know and/or change internal algorithmic functionalities (e.g. image restoration algorithms applied to raw data), vs. (ii) academic FR software packages.

4) **Related to other factors**, such as image quality (e.g., image resolution, compression, blur), time span (facial aging), occlusion, and demographic information (e.g., gender, race/ethnicity, or age). For example, a face recognition system will behave differently when it is trained and tested using a certain cohort (such as a race group) or when using different cohorts.

What is some of the up-and-coming technology that will be used in the future to deal with problems of recognizing unfamiliar faces and research in video biometrics?

Media giants such as Facebook, Google and Apple now include face detection and face recognition in their products (NIST 2011 report on Biometric Challenges). There are also discussions in the media on up-andcoming biometric technologies that will be used in the future to deal with various face recognition problems. Many of such technologies are expected to be low cost, such as cameras with built in face detection (many of the current smart phones already have this capability).

But, one of the current trends is the development of synergistic computer vision and sensing technologies to identify potentially hostile behavior and intent, with the purpose of uncovering clandestine foes. There is work in this area but not to the expected level of efficiency. In the future though such technologies will work better under more complicated scenarios and will have the capability to deal with large amounts of data - applied in video footage coming from any type of camera, e.g. surveillance, smart phones etc.

Could you name some quality metrics for practical facial recognition?

Before discussing about image quality metrics, it would be beneficial to discuss the importance of practical face recognition. When we are talking about practical face recognition, one of the things that comes into an operator's mind is data quality. We are interested in "image quality" of a biometric (face image) template (i.e. we ask ourselves "how noisy is this face image?").

However, we are also interested in the "matching quality" of such a template that is determined by computing the similarity score between a probe and a gallery (enrolled) face image. In either case we expect that high image and matching quality will result in high system performance - in other words, while a face image can be slightly blurry, sufficient noise can be removed so that face recognition performance improves .

The key is to understand that we need to (i) utilize existing (or design new effective) image quality metrics in order to reduce the number of poor quality face images acquired during enrollment and authentication and, as an effect, (ii) improve face matching performance. Thus, now we can focus on image quality metrics. Let me start by explaining the difference between "quality factors" and "quality metrics," terms used in image processing, for example, when trying to determine (quantify) the efficiency of an image restoration technique. "Quality factors" are considered to be image quality attributes such as sharpness, focus, contrast, brightness etc.

"Quality metrics," sometimes also called "image quality or distortion measures" are techniques that are used to quantify quality factors. Two typical image quality metrics are the peak signal-to-noise ratio (PSNR) and the Universal Image Quality index (UIQ) proposed by Wang and Bovik.

How can privacy concerns over facial recognition technology be alleviated amongst the general public?

We need to protect both National Security as well as Personal Privacy. I am not an expert in the area of privacy. But I can say that both the general public as well as the government, express concerns and have rights that should be mutually understood and respected.

Unfortunately, there is not any golden or magic solution that will make everybody happy. When national security is at stake (such as the tragic event in Boston), tough decisions need to be made. That is why access to public video footage was one of the keys to successfully deal with the apprehension of the Boston bombers and face images was an important identifier that was successfully used.

Now, on the other hand, unreasonable access to personal information, including biometrics data (including face images captured by surveillance cameras, cell phones etc.) is another problem and there are many decision makers that are working on this issue every day. And this is the good news.

The bottom line is that, while face recognition and biometrics in general, are not perfect, they can be beneficial to consumers in terms of security. Basically, biometrics, when properly used, offer greater protection on financial fraud and different types of theft (identity or data) since they are much more secure than using typical passwords and PINs.

You authored a paper on the "Applications of Passive Infrared Imaging to Forensic Facial Recognition." Could you share with us some of your research and findings on this paper or any others?

Below is a brief description of one of the most recent papers of MILab, i.e on "Applications of Passive Infrared Imaging to Forensic Facial Recognition."

"Within the last two decades, we have noticed improvement in the performance of visible-based face recognition (FR) systems in controlled lab conditions characterized by suitable lighting and favorable acquisition distances. However, over the years the technology has steadily progressed to tackling increasingly more realistic conditions, typically found in law enforcement or military operational environments, rather than adequately handling only well-controlled imagery.

Most related research emphasizes maintenance of high human recognition performance while coping with increased levels of image variability. Among the most insidious problems that visible-spectrum based face recognition systems need to tackle are (1) variation in level and nature of illumination, (2) the fact that as the level of illumination decreases, the signal to noise ratio rises quickly, and thus automatic processing and recognition become very difficult tasks, and (3) heterogeneous face recognition, i.e. dealing with probe (query) face images (captured using surveillance cameras operating in the infrared (IR) band) that need to be efficiently matched against visible band, good-quality face images (such as mug shots that may contain the face of the query subject) in order to establish the identity of different individuals.

While moving to passive IR FR systems, we need also to deal with other problems, including the cost of the sensors (there is a variety of imaging systems, from state-of-the-art bulky and expensive ones, down to lower quality, portable and less costly camera sensors) and efficient sensor usage to perform data collection
operations in a timely manner. In order to address the aforementioned problems in forensic face recognition, where human operators are necessary a part of the process, recent research has moved into the use of passive IR imagery (middle- and long-wave IR) and the development of alternative data collection systems as well as methodological approaches capable of performing eye detection and matching of heterogeneous face images. In this paper "Applications of Passive Infrared Imaging to Forensic Facial Recognition", a number of forensic thermal-based face recognition applications is discussed. The first one is an avatar-assisted application that can be used via a graphical user interface (GUI), primarily, for the collection of long wave infrared (LWIR) or thermal face images with minimum operator interference. The second one is an application that has the capability to

perform automated detection of human eyes in the passive IR band. The third application we developed has the capability to perform same spectrum (MWIR vs. MWIR) or cross-spectral (MWIR vs. visible) face matching.

In the first application, an integrated system is created that is capable of capturing the facial biometrics as well as physiological-based measurements (Photo-plethysmograph (PPG) and Electro-dermal Activity (EDA) of subjects during the course of an interview. The physiological-based measurements and thermal information of the facial regions are recorded and stored, while they can also be retrieved for further analysis using our designed and developed GUI that allows for easy operation. The second application was tested by performing a set of eye localization experiments.

The outcome of the experiments showed that human eyes on still full frontal, MWIR face images, can be detected with promising results. In particular, MILab's template-based eye detection technique achieved the best accuracy when using image templates that include both the eye and eyebrow regions (~91%). Finally, in the third application, we evaluated FR performance on holistic MWIR and visible face images and compared it against commercial and academic FR software. Experiments showed that images captured in the MWIR band can be efficiently matched to MWIR images, with the best results obtained when using our proposed FR approach.

We also determined that identification performance on MWIR imagery appears to be comparable to that of visible imagery (used as the baseline). However, as expected, cross-spectral experiments resulted in markedly reduced performance."

The lab has published many other papers in the area of FR and, instead of providing details of a selected number of papers, I would rather provide the lab's publication webpage so that our audience can have a look and even read some of those papers.

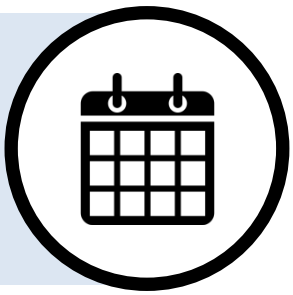
The link is: http://www.csee.wvu.edu/~tbourlai/publications/tbourlai.htm


CYBER
SECURITY

14 Strategies For Combating & Detecting Advanced Persistent Threats

Since 2014 cyber security incidents have risen **38%**.

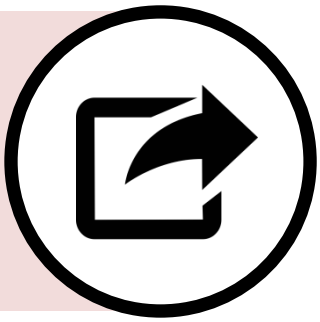
Before being discovered attackers often have **200 days**.



Cyber attacks cost the U.S. **$300 B – $ 1Trillion** a year.

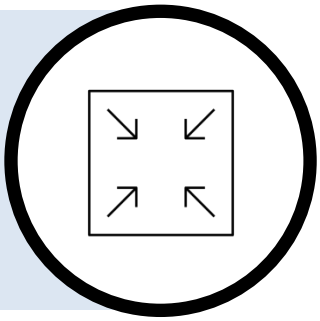
Advanced Persistent Threats (APTs) are some of the most dangerous and demanding challenges to computer security.

They've been known to steal valuable company intellectual capital and even government secrets. So, it's important to know if you've been targeted by one, and how to contain and combat the threat. Below Raed Albuliwi, Vice President of ANRC helps lay out the strategies for helping keep your network safe.



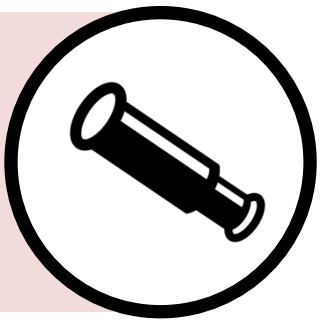
#1: Be weary of what you share.

Using publicly available information APTs can zone in on and collect it to help them zero in on the target network and users who may be near that network. Your website can become a tool for them to open the door to your sensitive information. Watch that you do not Some organizations have blindly uploaded network configuration diagrams showing the inner workings of their enterprise infrastructure or VPN authentication credentials for employees.



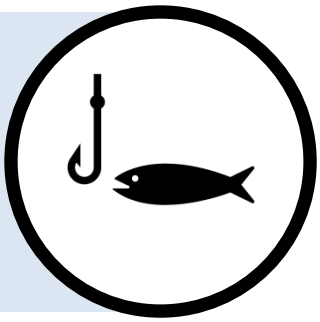
#2: Limit your attack surface.

Identify public critical information and limit/remove it. Attacks known as spearphishing attacks target individuals with their names, email addresses, titles …etc. Adjust your security posture to meet the risk requirements of having this information available.



#3: Monitor systems connected to the internet.

A potential adversary can be provided information, whether intentional or not, from your systems connected to the internet. The APT campaign starts here. Investing in a COTS solution to log this data and analyzing it should be getting done. If not, you're missing out on potential surveillance being conducted.



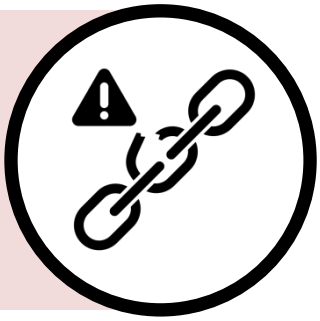
#4: Prepare for spear-phishing.

Spear-phishing is a tried and true method for circumventing the strongest network security infrastructures. one person to open the targeted email or click the malicious link in order to gain an initial foothold on your network.

Two strategies are listed below:

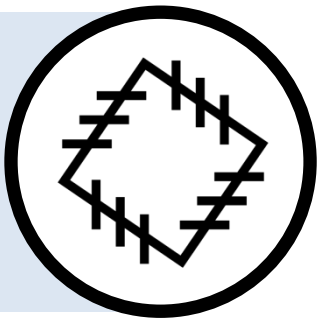
(a) Your own employees are the target for this. Make sure your organization employ computer security guidelines and best practices along with periodic training and audits.

(b) Leverage your existing technology. Within your email servers include aggressive filters to limit attachments that are not required for you to conduct your daily business activities. Also have scan for viruses using a COTS anti-virus solution.



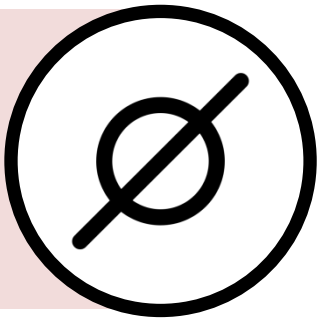
#5: Scan for vulnerabilities on your infrastructure.

Some well funded APT campaigns may have a dedicated group of individuals whose sole responsibility is to find unknown vulnerabilities. There are found in client software or the operating system itself. These zero-day vulnerabilities and exploits are sold on the cyber black market for large sums of money, sometimes in the tens of thousands of US dollars.



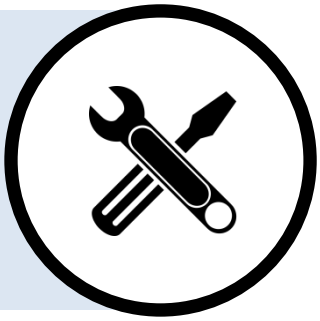
#6: Have an Enterprise Patch Management solution.

Protection against known vulnerabilities rests solely on a vendor getting a patch out as quickly as possible to its customers where it can be tested properly before being rolled out using an Enterprise Patch Management Solution. Employing updates across the enterprise is important, and the update procedure should be tailored to suit your organizations operational environment and production needs.



#7: Employ anti-zero day technology.

harden your hosts and networks against these types of exploits by investing in an antizero day protection system. APT intruders can only attack what they know about and are not expecting unique security solutions to be deployed on a target network.

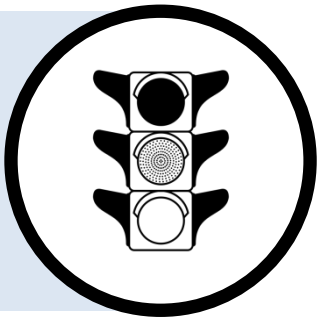


#8: Prepare for custom attack tools.

Being well-funded has its advantages and having tools that can bypass standard security solutions is a key differentiator between this threat and others. APT groups have the ability to develop and test their own hacking tools and malware.

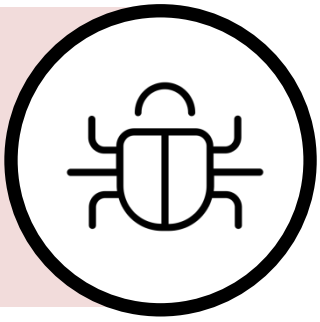
#9: Have a computer forensics and intrusion analysis team/individual.

Chances are APTs are embedded not only on the single exploited host, but have moved laterally throughout the network, infecting more hosts and servers, gathering passwords and information to further propagate throughout the network. It's important having a team that can work on performing a basic forensic of infected host(s) and gather unknown and suspicious binaries as well as restoring these systems.



#10: Utilize network traffic analysis.

Once you have an idea of which systems to investigate further, search for suspicious connections, services, programs and processes running that don't belong. Using the concept of auditing unknown binaries should help here. Look for programs that don't appear in your baselines and that are not digitally signed by a legitimate vendor (ex. Microsoft).



#11: Utilize malware analysis with a dedicated team

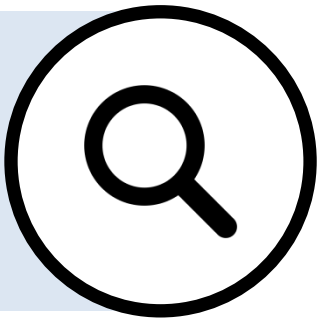
The simple fact is your traditional IT work force will be ill-equipped to fight this threat. Forwarding malware to an anti-virus vendor for signatures is not going to keep an APT intruder out of your network. Malware analysis can help you locate other systems compromised on the network that you might not already know about.

#12: Implement network security auditing.

In the case of the Chamber of Commerce intrusions, the APT attackers were able to acquire Administrator level credentials for the network, thereby allowing unhindered access across the entire network. Understand where information is being warehoused, and log all authorized and unauthorized access of this information.

#13: Squash phone home attempts.

Make sure your organization is in a position to flag suspicious connections to IP addresses sending large amounts of encrypted or enciphered data to unknown IP addresses. The goal of the APT is to maintain a long-term presence on the network, slowly leaking stolen information while remaining hidden. How do they accomplish this? They will likely use encryption and transfer the data over standard ports 80/443 which they know will not be firewalled off.



#14: Have a network anomaly detection system.

Make sure your organization is in a position to flag suspicious connections to IP addresses sending large amounts of encrypted or enciphered data to unknown IP addresses. The goal of the APT is to maintain a long-term presence on the network, slowly leaking stolen information while remaining hidden. How do they accomplish this? They will likely use encryption and transfer the data over standard ports 80/443 which they know will not be firewalled off

SUMMIT SESSION

Securing the Cyber Ecosystem with a National Cybersecurity Protection System

November 3 - 1600

anonymous by parkjisun from the Noun Project; Calendar by Edward Boatman from the Noun Project; Money by Creative Stall from the Noun Project; Zoom In by Juan Pablo Bravo from the Noun Project; spyglass by George Bourletsikas from the Noun Project; Fishing by Edward Boatman from the Noun Project; broken chain by Andrew Forrester from the Noun Project; patch by Christina W from the Noun Project; Empty by Rflor from the Noun Project; Fingerprint by Daouna Jeong from the Noun Project; Traffic Light by Nikita Kozin from the Noun Project; Bug by Gregor Črešnar from the Noun Project; Lock by Simple Icons from the Noun Project; Telephone by Megan Mitchell from the Noun Project; Magnifying Glass by marcel grödl from the Noun Project

DoD Looks to Private Sector for Cyber Security Partnerships

By John M. Doyle

With every passing week, the necessity – and vulnerability -- of cyberspace becomes more apparent. Hardware and software failures on the Bloomberg LP network forced its iconic trading terminals to go dark for several hours on April 17 and financial markets across much of the globe ground to a halt. The private correspondence of top executives and personal data of thousands of employees at Sony Pictures were revealed to the world last year by North Korean hackers after the movie company released a comedy about a plot to assassinate the dictatorship's leader. The data was published again by WikiLeaks in mid-April.

The secret government collection of telephone data was exposed, embarrassing the National Security Agency and the Obama administration after rogue NSA contractor Edward Snowden downloaded volumes of files and leaked many to the media before fleeing the country. And most recently, hackers, traced to Russia, penetrated an unclassified Pentagon network earlier this year before they were detected, identified and expelled. "They discovered an old vulnerability in one of our legacy networks that hadn't been patched," Defense Secretary Ashton Carter told an audience at Stanford University April 23.

The revelation came as Carter unveiled an updated version of the Defense Department security strategy for cyberspace. While the technology advances developed in Silicon Valley and elsewhere have made many things in modern life "easier, cheaper and safer," Carter noted that "it's become clear that these same advances and technologies also present a degree of risk to the businesses, governments, militaries, and individual people who rely on them every day … making it easier, cheaper, and safer to threaten them. The same Internet that enables Wikipedia also allows terrorists to learn how to build a bomb."

The threat comes from state and non-state actors alike, Carter said. "Just as Russia and China have advanced cyber capabilities and strategies ranging from stealthy network penetration to intellectual property theft, criminal and terrorist networks are also increasing their cyber operations," he added.

The new strategy details what the Pentagon's cyber missions are and what the United States will do to protect its networks and respond to those who try to damage them. The 30-page strategy (also summarized later in this eBook) focuses on building cyber capabilities and organizations for the Defense Department's three primary cyber missions: Defending the department's (DODS) networks, systems and information; defending the U.S. homeland and U.S. national interests against significant cyberattacks; and providing cyber support to military operational and contingency plans.

To accomplish those missions, the first task is to build up the DOD's Cyber Mission Forces: the people who will hunt down intruders, test U.S. networks with red-team attacks and perform the forensics to keep the systems secure.

The strategy envisions 13 National Mission Teams to defend the United States and its interests against cyberattacks of "significant consequence," which Carter described as acts that would cause loss of life, property destruction or a serious negative impact on foreign policy or the national economy.

The strategy also calls for 68 Cyber Action Teams to defend priority DOD networks and systems, against priority threats; 27 Combat Mission Teams, to support the operational plans and contingency operations of the nine Unified Combatant Commands, like U.S. Central Command and Transportation Command; and 25 Support Teams to provide analytic and planning support to the National Mission and Combat Mission teams.

"We're just beginning to build and imagine this cyber force in DOD," Carter said. Because American businesses own and/or operate about 90 percent of U.S. networks, the private sector must be a key partner, both in protecting its own data and networks and forging partnerships with government to exchange information and talent. Navy Admiral Michael Rogers, the chief of both National Security Agency (NSA) and U.S. Cyber Command, sounded a similar note before Congress last year. "The challenges here are so broad, that the idea that one sector or one individual organization is going to solve this, I just don't think is realistic," Rogers told the House Intelligence Committee, last November, adding: "It is going to take a true partnership between the private sector, the government and academia to address the challenges we have."

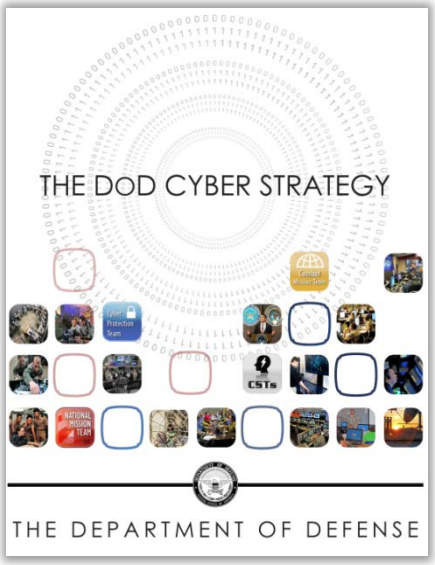
Operationalizing cyberspace in the future "is all about people and partnerships," Rogers told a seminar last year on Cybersecurity needs by 2025 hosted by the Association of the U.S. Army. The Department of Defense, he said, is not on the cutting edge when it comes to developing information technology. "We are a user of technology that is largely generated by individuals and organizations that reside outside the DOD," Rogers said, adding that he didn't think that trend would be changing between now and 2025.

An Army National Guardsman discusses ways to make the exercise more challenging for cyber defenders with a fellow team member from the Air National Guard during the 2014 Cyber Shield exercise at the National Guard Professional Education Center, North Little Rock, Ark. U.S. Army Photo/Staff Sgt. Kelvin Green

STRATEGIC GOALS

for Cyber Security

The Department of Defense recently outlined its Cyber Security Strategy, including the strategic context of cyber operations, the department's goals for Cyber going forward, and the implementation objectives. We've parsed their strategy document to pull out at-a-glance quotations for your benefit. Make sure to view the full DoD cyber strategy document to get the big picture.



STRATEGIC GOAL I: "BUILD AND MAINTAIN READY FORCES AND CAPABILITIES TO CONDUCT CYBERSPACE OPERATIONS."

In order to effectively police the digital realm, the DoD needs highly trained personnel to catch problems before they grow and combat them as they develop—ready at a moment's notice.

ACTION POINTS FOR GOAL I:

- Build the cyber workforce
- Build technical capabilities for cyber operations
- Validate and continually refine an adaptive command and control mechanism for cyber operations
- Establish an enterprise-wide cyber modeling and simulation capability
- Assess Cyber Mission Force capacity

STRATEGIC GOAL II: "DEFEND THE DOD INFORMATION NETWORK, SECURE DOD DATA, AND MITIGATE RISKS TO DOD MISSIONS."

The crux of this goal consists of prioritizing the most critical networks to defend (as it's nigh-impossible to defend all networks due to the size of the task), and then to shore up those networks by investing in innovative solutions and working with the private sector to achieve excellence.

ACTION POINTS FOR GOAL II:

- Build the Joint Information Environment (JIE) single security architecture.
- Assess and ensure the effectiveness of the Joint Force Headquarters for DoD information network (DoDIN) operations
- Mitigate known vulnerabilities
- Assess DoD's cyber defense forces
- Improve the effectiveness of the current DoD Computer Network Defense Service Provider (CNDSP) construct in defending and protecting DoD networks
- Plan for network defense and resilience
- Red team DoD's network defenses
- Mitigate the risk of insider threats
- Exercise to provide Defense Support of Civil Authorities
- Define and refine the National Guard's role in supporting law enforcement, Homeland Defense, and Defense Support of Civil Authorities missions
- Improve accountability and responsibility for the protection of data across DoD and the DIB
- Strengthen DoD's procurement and acquisition cybersecurity standards
- Build collaboration between the acquisition, intelligence, counterintelligence, law enforcement, and operations communities to prevent, mitigate, and respond to data loss
- Use DoD counterintelligence capabilities to defend against intrusions
- Support whole-of-government policies and capabilities to counter intellectual property theft

STRATEGIC GOAL III: "BE PREPARED TO DEFEND THE U.S. HOMELAND AND U.S. VITAL INTERESTS FROM DISRUPTIVE OR DESTRUCTIVE CYBERATTACKS OF SIGNIFICANT CONSEQUENCE."

The Department of Defense must create new partnerships with other agencies—and work within the partnerships they already have—to avoid stovepiping and work towards the common goal of mitigating malicious cyber attacks before they can impact U.S. interests.

ACTION POINTS FOR GOAL III:

- Continue to develop intelligence and warning capabilities to anticipate threats.
- Develop and exercise capabilities to defend the nation
- Develop innovative approaches to defending U.S. critical infrastructure.
- Develop automated information sharing tools.
- Assess DoD's cyber deterrence posture and strategy

STRATEGIC GOAL IV: "BUILD AND MAINTAIN VIABLE CYBER OPTIONS AND PLAN TO USE THOSE OPTIONS TO CONTROL CONFLICT ESCALATION AND TO SHAPE THE CONFLICT ENVIRONMENT AT ALL STAGES."

The DoD must invest care in creating not only security standards and defensive protocols –but also in creating integrated options which could be utilized offensively against an enemy's communications, military infrastructure, and weapons capabilities.

ACTION POINT FOR GOAL IV:

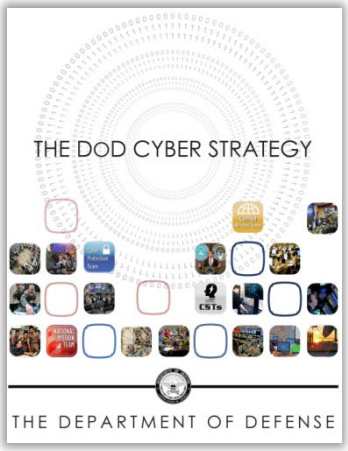
- Integrate cyber options into plans

STRATEGIC GOAL V: BUILD AND MAINTAIN ROBUST INTERNATIONAL ALLIANCES AND PARTNERSHIPS TO DETER SHARED THREATS AND INCREASE INTERNATIONAL SECURITY AND STABILITY.

Two of the other objectives deal with building relationships with the private sector and with other agencies… this one deals with facilitating cyber cooperation internationally, including in the Middle East, the Asia-Pacific, and the members of NATO.

ACTION POINTS FOR GOAL V:

- Build partner capacity in key regions
- Develop solutions to counter the proliferation of destructive malware
- Work with capable international partners to plan and train for cyber operations
- Strengthen the United States cyber dialogue with China to enhance strategic stability



READ THE FULL DEPARTMENT OF DEFENSE CYBER STRATEGY

11TH ANNUAL HOMELAND SECURITY WEEK

JOIN US

IN WASHINGTON D.C.

The 11th Annual Homeland Security Week taking place November 1-3 will bring together top homeland security leaders from government, industry and academia alike to take a deep dive into current challenges and future requirements necessary for numerous government agencies, all directly or indirectly responsible for U.S. homeland security, to facilitate a complex, joint, multilayered plan to combat the evolving challenges our country faces.

LEARN MORE