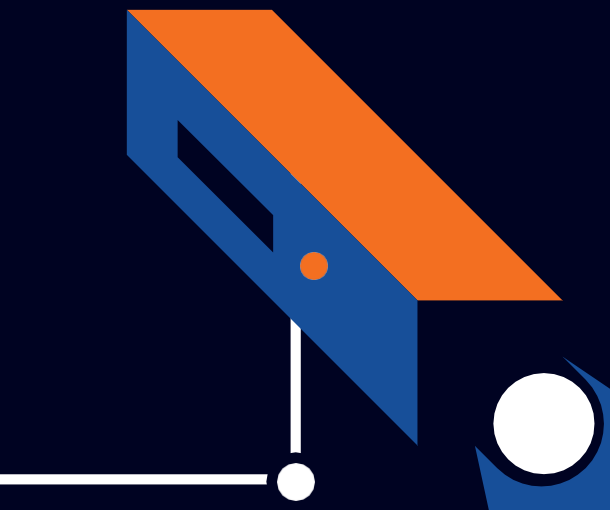
WHITEPAPER

\Orchestrating a brighter world NEC



HOW DIGITAL TECHNOLOGY *CAN BE THE DIFFERENCE* IN MAKING CITIES SAFER

CONTENTS

Contributors

Walter Lee
Evangelist and Government Relations Leader
NEC Global Safety Division

Kris Ranganath
Vice President, Technology & Solutions
Advanced Recognition Systems
NEC Corporation of America

Chapter 1

NEW CHALLENGES FROM NEW THREATS

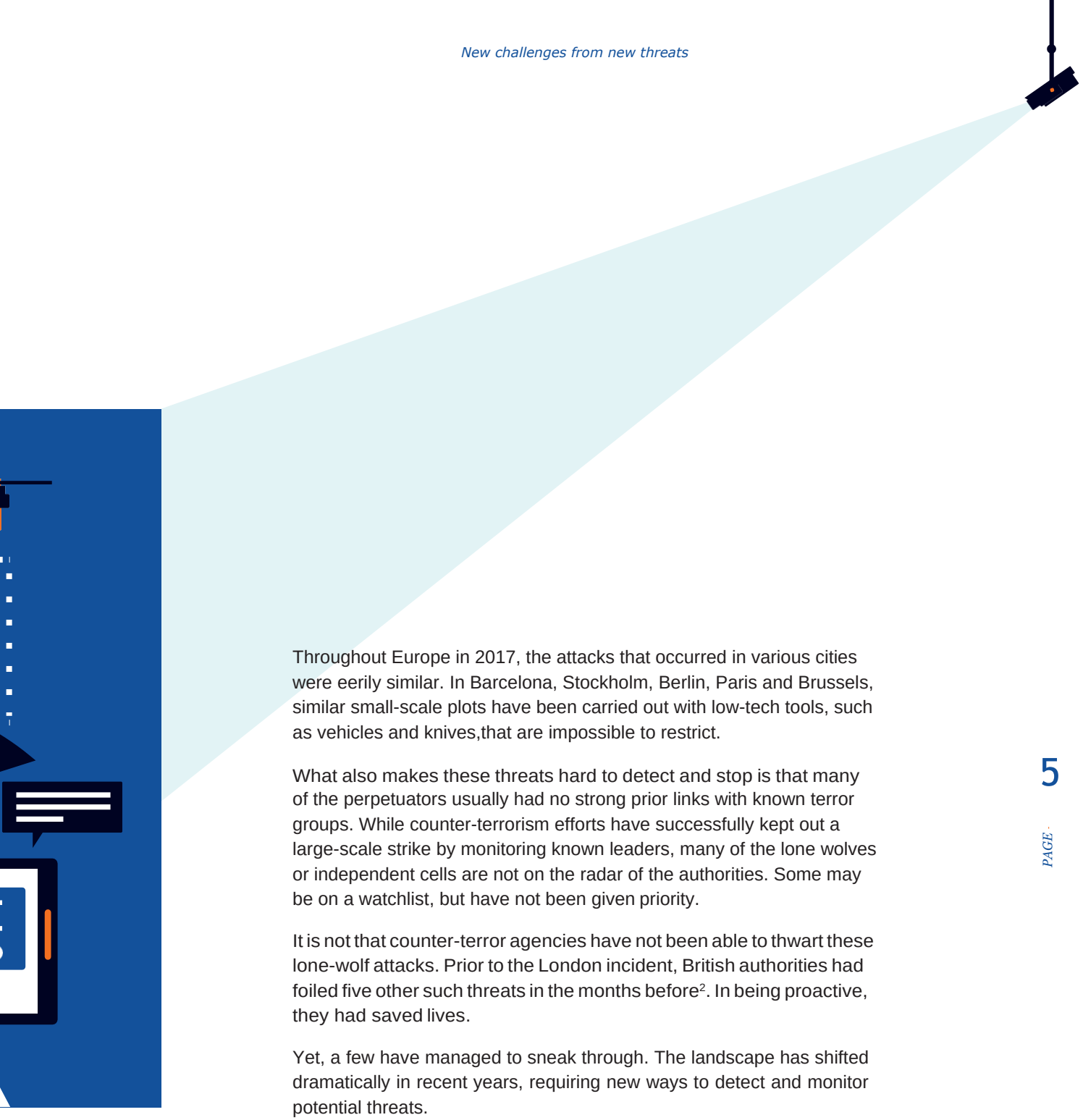
On September 11, 2001, the world changed with the devastating attacks on the World Trade Center in the United States. In the years after, the threat from terrorism has also morphed. As more resources have been poured into fighting terror, so have the tactics of terrorists changed.

While the 9/11 attacks were planned meticulously and executed by men trained for the deadly task, many of the attacks in recent years have been carried out by so-called lone wolves. They may be smaller in scale but harder to detect and prevent.

In eight deadly minutes in June 2017, three attackers slammed a van into people on the crowded streets near London Bridge, then went on foot knifing anyone they saw. They killed eight people and injured 48 others in the short time they were rampaging, before being stopped by police[1].

In the few months before, a similar attack was mounted with a vehicle ramming through the Westminster area in London. And a bomb detonated during a concert in Manchester in the same year killed another 22 people.

1 http://www.independent.co.uk/news/uk/home-news/london-attack-live-updates-news-bridge-terror-borough-market-stabbing-van-victims-jihadi-killed-a7772851.html
2 https://www.vox.com/world/2017/6/5/15739168/london-attack-terrorism-counterterrorism



Throughout Europe in 2017, the attacks that occurred in various cities were eerily similar. In Barcelona, Stockholm, Berlin, Paris and Brussels, similar small-scale plots have been carried out with low-tech tools, such as vehicles and knives,that are impossible to restrict.

What also makes these threats hard to detect and stop is that many of the perpetuators usually had no strong prior links with known terror groups. While counter-terrorism efforts have successfully kept out a large-scale strike by monitoring known leaders, many of the lone wolves or independent cells are not on the radar of the authorities. Some may be on a watchlist, but have not been given priority.

It is not that counter-terror agencies have not been able to thwart these lone-wolf attacks. Prior to the London incident, British authorities had foiled five other such threats in the months before[2]. In being proactive, they had saved lives.

Yet, a few have managed to sneak through. The landscape has shifted dramatically in recent years, requiring new ways to detect and monitor potential threats.

Today's terror groups have changed by using digital technology, much like how companies and governments have embraced digital transformation. Though they have been disrupted over the years, they have now turned to commonly available technology to change the game.

Drones, for example, have been used in asymmetric warfare. Forces fighting against ISIS in Iraq came across flying machines flown by the insurgents to carry out surveillance and even drop small explosives on them[3]. For years, anti-terrorism agencies have feared a drone could be used by terrorists against targets in a city.

3 http://www.newsweek.com/isis-air-force-army-drones-drop-bombs-585331

The Internet's reach has changed the equation as well. Using social media to great effect during its heyday in 2016, ISIS swelled its ranks by attracting many young people to join its cause, including those who know nothing about the religion it claims to represent. Today's competing jihadist groups regularly compete for prestige and power online by releasing incredulous claims and presenting gruesome videos of victims caught in their crosshairs.

At the same time, some extremist groups that have been largely ignored by counter-terrorism agencies are also recruiting through online channels. Right-wing white supremacist groups, for example, have been able to drum up hate and incite individuals to carry out brazen attacks. Many such extremists have no previous history with law enforcement.

What this means is that the scope has drastically widened for counter-terrorism agencies. There are more individuals who may potentially threaten a city's safety than the regular suspects who are likely to be under intense scrutiny.

Spotting a plot early

In many lone wolf attacks, there have been clues to an individual's potential for plotting an attack[4]. He may have loitered at a target location before finally committing the act. He may have been noticed in regular online chatrooms and forums boasting about carrying out an attack. The Las Vegas shooter in 2017 bought 33 guns in the 12 months before the incident, though he had a license to do so[5].

Collaboration across agencies, borders

Inter-agency collaboration[6] is key today to finding such lone wolf attackers. The sharing of intelligence on a common platform needs to accelerate in future. Private-public collaboration will make a difference, with data collected by citizens shining a light on areas otherwise not identified as threats.

4 https://www.theguardian.com/news/2017/mar/30/myth-lone-wolf-terrorist
5 https://www.usatoday.com/story/news/nation/2017/10/04/las-vegas-shooter-bought-33-guns-last-12-months/730634001/
6 http://www.independent.co.uk/news/world/middle-east/uk-anti-terror-israel-lone-wolf-attacks-help-islamists-advise-westminster-palestinians-london-bridge-a7817286.html

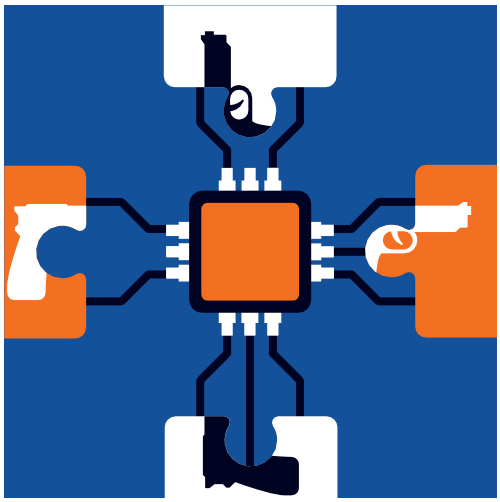
Without a doubt, the number of attack vectors has increased. Besides physical targets, terrorists can turn on the increasingly digitized city services to wreak havoc. The use of sensors in a city gives it more eyes and ears, yet they require security to ensure they work in an emergency. They also have to be protected from cyber attacks that may compromise the data they produce.

For example, sensors used to measure water levels could be sabotaged via a cyber attack, so that a flood would not be detected and alarms not raised.

This calls for a rethinking of security solutions, from border control to city surveillance. The next generation has to better knit together a picture of a potential attack before it happens. The leads have to come from both cyber and physical. Intelligence should be gathered from both digital and human channels.

Need for data analysis

More data alone may not always help. With limited manpower already deployed for existing operations, there has to be a new way to find useful clues from the data collected, say, from online chatter, browsing patterns or social media. Where a team of humans do not have the capacity to do so, artificial intelligence (AI) could augment them.



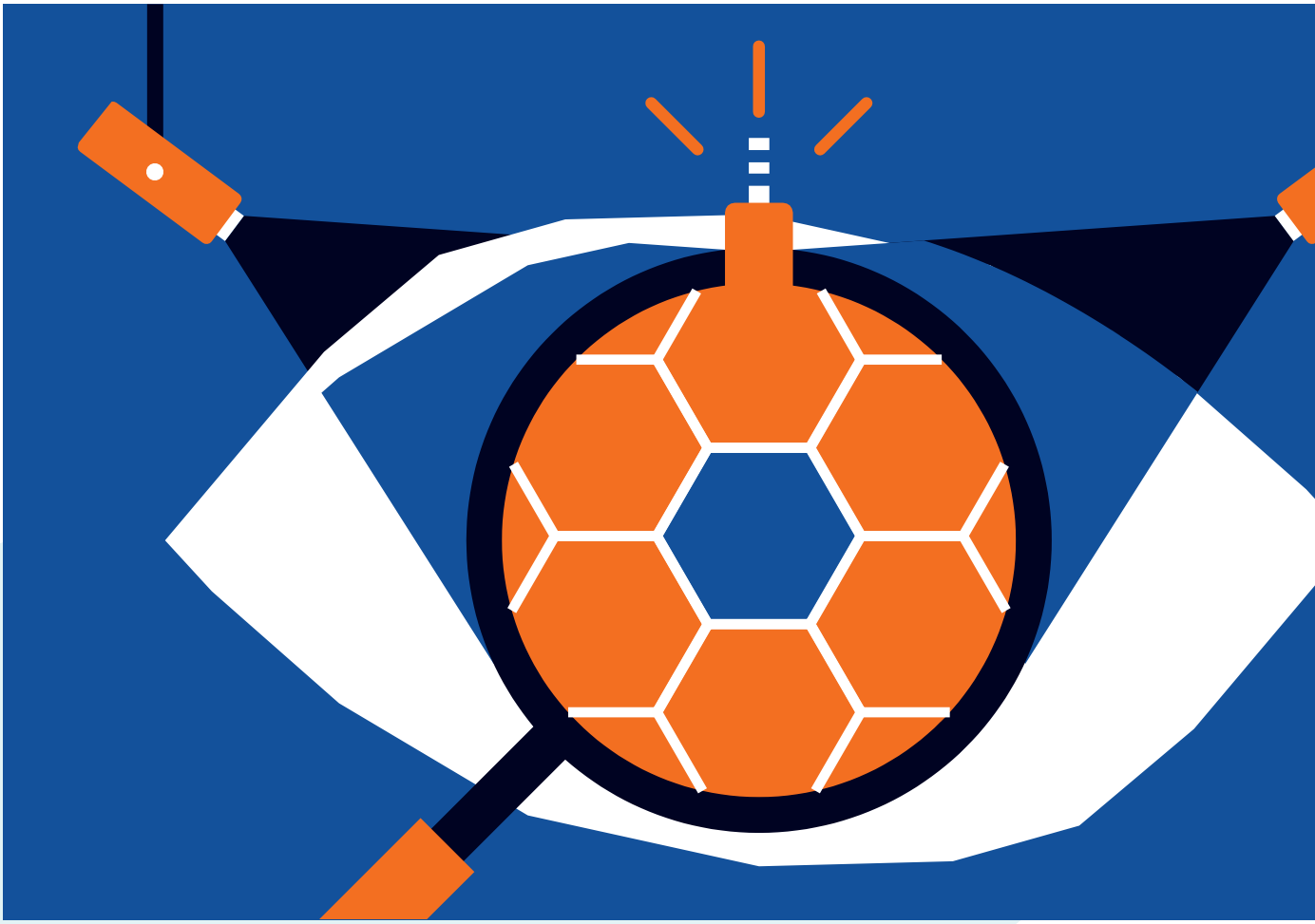
AI to bring the pieces together

For better situational awareness, upgraded counter-terrorism technology will be important. In the same way corporations are learning more about their marketplace through digitalization, so can law enforcement agencies unearth hidden threats to a city.

The need is made more urgent because threats are becoming less predictable. Just as potential attackers have taken to new technologies to up their game, counter-terrorism teams have to evolve the way they access threats and stop attacks.

Chapter 2

SENSING THREATS PROACTIVELY



Finding and following up on leads that may point to a potential attack are the toughest tasks in stopping many lone wolf plots. Crucial to this is sifting the real information from the noise and chatter online.

One of the London Bridge attackers of 2017 was filmed in a British documentary unfurling an ISIS flag and being involved in an altercation with police officers a year before the incident.

Earlier, in 2014, the extremist who held people in a Sydney café hostage had been out on bail following charges for sexual assault. He had also been observed at protests against counter-terrorism police operations and for putting up offensive posts on Facebook.

The clues are often easy to pick up on hindsight. But what if the authorities could find the right cues to follow up by examining and predicting these plots more accurately? Terrorism often manifests in an overt act of violence, but its intention is one thing that is hard to detect.

What if there is a way to map out a possible sequence of activities, from an attacker's passive radicalization to active involvement online to the

7 http://www.express.co.uk/news/uk/813075/london-bridge-terror-attack-identity-attacker-ISIS-channel-4-documentary

actual acting out of the extremist agenda? This could help stop it from being taken to a deadly conclusion.

To be successful, surveillance is needed in both the digital and physical spaces. Online, cyber information surveillance combs the vast database of information online to locate useful intelligence on cyber space that may provide clues to a group of attackers. One of them may have posted on social media of an “important” event it was planning. Another could have been visiting websites showing how to handle weapons, for example.

Physical surveillance, no doubt, will be just as important as before. A person may have been scouting an area, say, to drive a van through or plan his route of attack on foot afterwards. An attack that is pre-planned, even in a short run-up, is something that counter-terrorism forces can detect. Cameras may pick up the suspicious behavior, but the video has to be analyzed for it to become actionable intelligence.

Key to this sensing is the ability to gather data from various sources to assess if a person is likely to commit a violent act. His behavior on social media alone may not signal that. However, the situation may change if other information, such as his purchase of powerful rifles, travel pattern (at border control), and criminal records are pieced together to form a more coherent picture.

In other words, sensing cannot be done in silos. One aspect of a person’s public life may not be enough to show an intention to carry out a plot. But several red flags placed together, showing their context better, might offer a different perspective.

For example, the shooter at a nightclub in Florida in 2016 was a security guard who had a firearms license to buy the guns he used to kill 49 people and injure another 53. He had twice been investigated by the authorities for suspected terrorist sympathies, yet was still allowed to buy high-powered rifles[8].

Improved sensing in future would have to put the pieces of a puzzle together much better. For this to happen, inter-agency cooperation will be key. AI will be even more important in the years ahead. Before that, the sharing of intelligence and leads has to happen, to assist law enforcement to more accurately triangulate and zoom in on a likely terrorist.

Indeed, a better mechanism to share criminal data among agencies as well as an integrated intelligence platform for the police were two recommendations for Australia after the Sydney attack[9].

8 https://www.theguardian.com/us-news/2016/jun/13/orlando-nightclub-massacre-suspect-fbi-guns-buy
9 http://www.smh.com.au/nsw/the-45-recommendations-of-lindt-cafe-siege-inquest-20170524-gwc00o.html

Chapter 3

INTELLIGENCE THROUGH ADVANCED SURVEILLANCE

Key to the effort is an advanced city surveillance system, along with a command and control center that has the information analyzed quickly and accurately. If a terror attack does occur, how law enforcement and counter-terrorism agencies respond will make an important difference to the outcome.

In the London Bridge attacks, armed police officers arrived on the scene within eight minutes and shot the three terrorists stabbing innocent victims on the street. Yet, the short span of time was enough for the attackers to kill and maim.

Sometimes, the best chance of stopping an attack is in the minutes just prior to it, through city-wide surveillance and data analysis. With the live video feeds coming through online cameras, it is important that the authorities get the intelligence needed.

Surveillance will be more effective if it can triangulate three criteria – the person, place and time of interest. It must be able to make sense of the context provided by the raw data captured on video cameras.

If a person on a watchlist turns up at a high-profile area, say, a parliament building and a time when

the government is meeting, it could mean that the possibility of an incident could be higher than usual. An alert has to be sent out at a higher level than if one or two of the criteria are met.

This could mean the difference between foiling an imminent attack and having the information being missed in a sea of data flooding in today.

In Tigre, Argentina, for example, the city authorities have developed a 22-seat command and control center that links up various components such as street surveillance, vehicle tracking and force coordination. From the Tigre City Operations Center, officers can view incoming information from CCTV cameras, intelligent video analysis and other data.

Street surveillance also enables officers to detect suspicious behavior. For example, someone loitering in a sensitive area for a period of time would automatically trigger an alert to an officer to follow up and take action. At the same time, license plate recognition and tracking across cameras will let officers follow a person of interest and possibly prevent an attack.

This has to happen in real time. To do so, new ways are needed to process the enormous amounts of data, for example, to recognize faces and behavior in a video and coordinate between agencies to take action.

In India's Surat City, a face recognition system was launched in 2015 to match faces against a watch list of individuals in real time. Once a person of interest is located, an alert is triggered for officers to follow up. The match is done by enhancing the poor quality inherent in some pictures from existing video surveillance systems.

Besides fixed systems, police officers will in future also have access to live body-worn cameras that bring real-time feeds to increase situation awareness. Unlike current body-worn cameras which are usually not transmitted live, police officers could have their cameras connect wirelessly to a nearby hub, possibly a police vehicle, which then runs a quick face recognition algorithm to check if a person is one of interest[10].

Simply by looking at a person "through his camera", an officer can be given live, accurate information on a suspect. He would not have to radio back separately.

He is also literally the "eyes and ears" of a preventive effort, if the data can be employed for real-time predictive analysis. Even if the officer misses suspicious behavior, say, a car circling a building repeatedly, video analysis in the back-end can pick that up and alert the authorities to take action.

How all the information is used is key to preventing and, if needed, responding effectively to a terrorist attack. AI could be key in future, to assist human operators.

10 http://sg.nec.com/en_SG/press/201708/20170815_01.html

Chapter 4

SMART BORDER CONTROL

All this advanced sensing and surveillance will be important not just in the city, but also at airports and other points of entry. Border control has to be equipped with the same sensing capabilities and access to a centralized trove of data to monitor the entrance and exits of people going through the border.

Does a person coming in have a criminal record? How many times has he been here? If he is a local citizen, is he on any watchlist?

While a lot of lone wolf attackers are locally radicalized, some may have travelled to overseas battlegrounds to fight with other insurgents or receive military training. This is where border control plays a big role in monitoring persons of interest passing through the gates at an airport, for example. To do that, the first order of business is to identify a person correctly.

Increasingly, smart passports with a secure chip containing biometric information, such as fingerprints, are making it easier for immigration authorities to confirm if a person is who he says he is. When a person reaches a checkpoint, he is asked to compare his fingerprint on the spot against the one which is stored on the passport chip. If he confirms his identity, he is allowed to go through.

Some countries, require travelers to scan their irises as well, as an additional measure. This means a country can store various biometric information of a person entering a country. In identifying someone, the more information that is collected, the more accurate it can be.

Facial recognition is another growing form of biometrics used at entry points. With increasingly accurate and fast recognition with today's technology, it is becoming a non-intrusive yet effective way to identify or find a person in a crowd.

In airports in Chicago, Washington and Texas in the United States, the technology has been used as an additional step to verify passengers' identities[11]. Going beyond that, some airports also turn to liveness checks to detect if someone is attempting to trick a face recognition system by wearing a mask or putting on a disguise, for example.

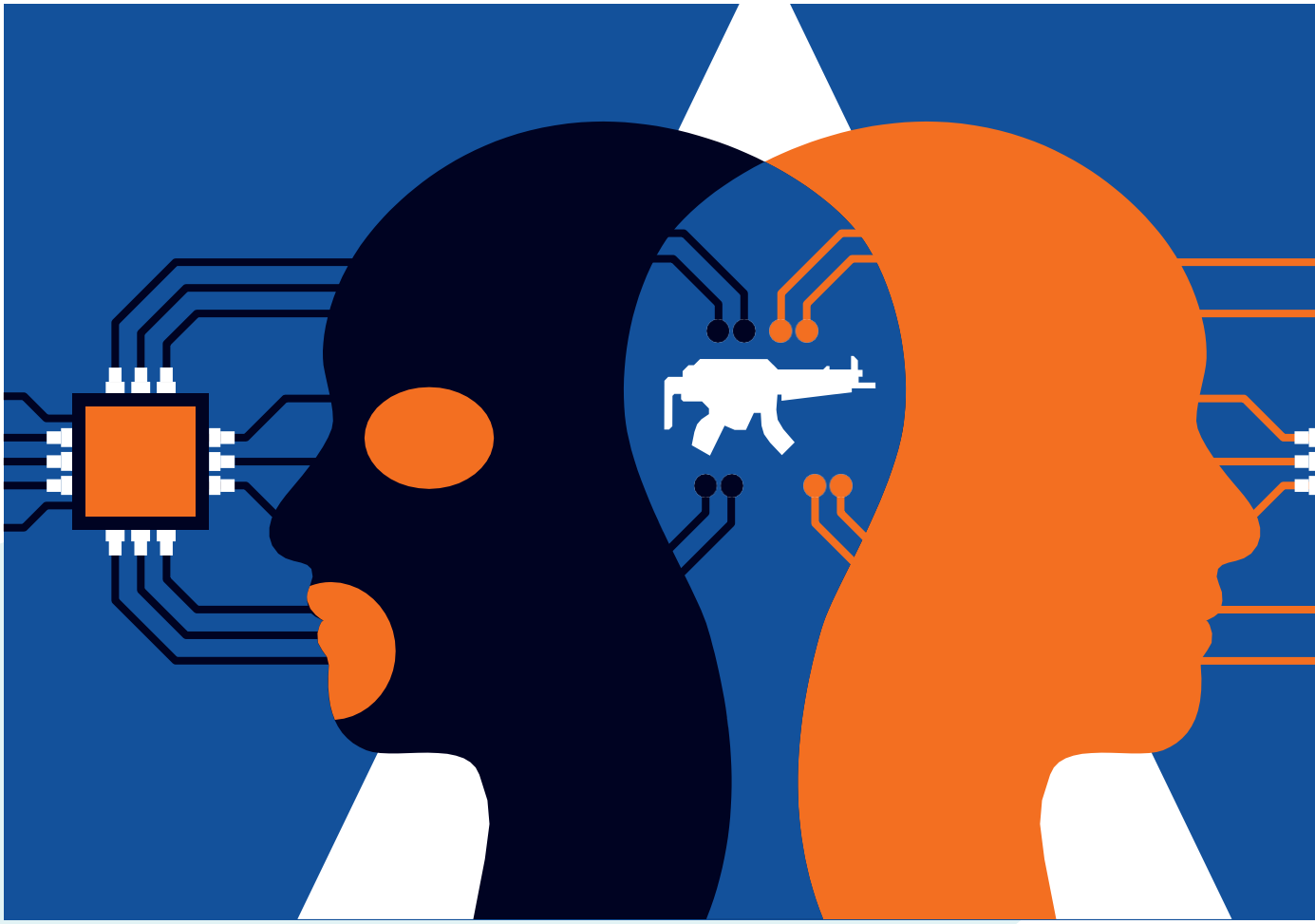
Liveness enables a face recognition system to look for key features, such as skin texture and colour and light reflection that it has "learnt" from analyzing thousands of previous photos. This way, a machine can aid human operators at a border by looking out for persons of interest.

Already, Liveness technology has been deployed in Hong Kong. Various detection methods can be used in this regard, but key to many border control systems is the ease of use and compatibility with existing systems. This will enable Liveness-enabled face recognition systems to quickly get on the job to prevent terrorism suspects from entering a country.

11 http://www.chicagotribune.com/news/local/breaking/ct-face-scans-ohare-0720-20170719-story.html

Chapter 5

THE PROMISE OF ARTIFICIAL INTELLIGENCE



Underpinning much of the evolution of modern counter-terrorism technology is AI. One important job it performs is to unify information collection, control and distribution, so that human operators will get to all the intelligence needed to make a decision or leap into action.

In sensing an attack accurately, AI could be the difference needed to stop it. As a hub for all the information flowing in, it can play the role of a "virtual agent" to human operators, by making sure they do not miss the big picture while trying to piece together a puzzle.

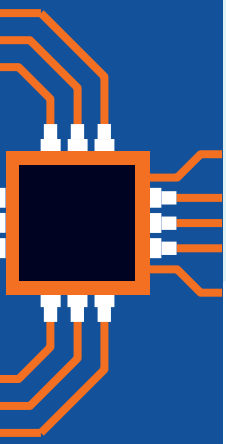
If a person tries to buy a bulletproof vest, AI may flag that as a significant incident. If he is also a person of interest on a watchlist or with a record of violent crime, he might be flagged again as a higher risk than usual. When he next tries to buy, say, 30 guns and thousands of rounds at a go, his importance to the authorities will be flagged as urgent. Investigators can then be tasked to immediately check up on him.

Essentially, AI can keep sensing all the sensing points that humans may miss or don't have the capacity to process. The AI engine can also keep looking for changes in behavior, so if it has good

reason to believe that something is wrong, it can flag a suspect to investigators, even if they may have okayed him in the past.

AI could also enable a continuous vetting process. This means people in sensitive environments, say, pilots or guards in an airport or trusted officers in the military, may be subject to vetting on the job. For example, employers running critical infrastructure in the US are notified if a staff member is arrested for a federal crime. In future, AI can do this automatically for all roles that require sensitive access to equipment or infrastructure.

Despite all the pre-emptive effort, what happens if a crisis does occur? AI can play a crucial role in a fast-changing situation. In Japan's Toshima City, for example, a disaster control system takes the input from 51 cameras in emergency relief centers, near major facilities and major roads and compiles the data on a map to help visualize a developing emergency, such as an earthquake.



> It also helps by analyzing crowd behavior to see if there are stranded commuters. Overcrowding or stagnation might also prompt a human operator to react to a fast-changing situation much more effectively.
>
> Though the real-time system is used for emergency purposes, it is suited to counter-terrorism uses as well. In detecting unusual behavior, for example, a crowd running away in one direction or mass panic and stress, an alert can be sent to a commander at a crisis center.
>
> Law enforcement officers may be guided through the AI-assisted geospatial system if they have to confront attackers on the run in the streets. The use of robotics and drones in future could also add to the mix of real-time systems in use during a terror attack.
>
> Today's AI can take information not just from official sources but also those from citizens. Smartphones held by citizens provide vital clues to finding and stopping terrorists in their tracks during an attack. Through apps on their mobile devices, a user can press a panic button to inform the authorities without even calling the police on the phone. If enough people trigger an alert at a certain location, a command center can be warned much more quickly.

The centralized system will have to be able to take in various sources of data. External sources can be in the form of video and audio sent from cameras, triggered by suspicious behavior detection or the sound of gunfire, for example. Sensors detecting fire, smoke or toxins may also sound the alarm.

Perhaps more importantly, the system should be able to assign a criticality to each event that is reported. This helps prioritize the management of each incident, helping take the guesswork out of a human operator who may otherwise be overwhelmed with data.

With Standard Operating Procedures (SOPs) in place in the system, each operator will also respond to an incident with an action plan. In some emergencies, such as when a likely terrorist attack is detected, all the relevant operators, say, armed police officers located near the incident, may be activated automatically to respond.

In such cases, AI enables a swifter, more effective reaction. No longer encumbered by having to analyze the increasing flood of data coming through in real time, decision makers and commanders can focus on an operation against a terrorist attack or preempt one before it begins.

Chapter 6

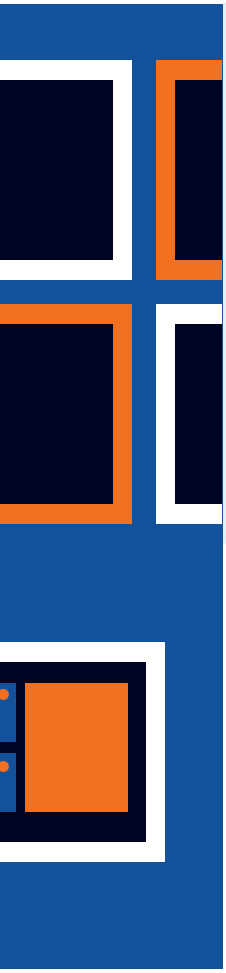
COUNTER-TERRORISM EVOLVES

In the 1970s and 1980s, terrorists often plotted to take hostages in prominent buildings or on planes. Their key objective was to draw attention to their struggle. They sometimes sought the release of comrades held in prisons by governments around the world.

In the 2000s, the modus operandi has become more deadly and unpredictable. One goal has been to kill or maim as many people as possible. Most recently, terrorists have turned to low-tech equipment and become harder to stop.

This comes as ISIS loses ground in key battlefields in the Middle East. It has called for these self-styled attacks through social media and other channels, inciting hatred and inspiring more attacks. To counter this changing threat, security agencies have to evolve as well.

AI brings unprecedented speed to the flow and analysis of information, making decisions and reactions much faster. This is one important game changer for counter-terrorism agencies looking to become more effective.



Just as corporations around the world have sought to digitize their operations and understand their customers better, city authorities have to bring all the information at hand to bear. The difference could be mere minutes in terms of reaction time, but that could matter so much, as the recent attacks in Europe suggest.

Technology could do one of three things today – support, extend or hinder. Secure wireless communications will support a police officer on the street. Surveillance cameras can monitor a wider area, extending them physically empowering them as well. In this case, human operators have to be careful not to relinquish their responsibility.

What agencies have to be careful about is technology hindering their work. For example, officers wearing on-body cameras may turn them off because they feel the technology does not help in their everyday asks. This could lead to unintended effects and diminish the benefits of new deployments.

The deployment must be constructed to support the concept of operations (CONOPS), that is, the body-worn cameras or any other tools must support existing CONOPS.

The good news is technology can be deployed much more easily, even in an ad hoc manner, to fit an operation today. During the Champions League Final in Cardiff, Wales in 2017, shortly after the attacks in the London, the local police stepped up its real-time video surveillance with cameras mounted on police vans[12].

Using face recognition technology, it could locate persons of interest on pre-determined watchlists, including criminals, suspects and others. A man who was wanted for a recall to prison managed to walk past several officers on a main street before it was spotted by a camera and identified. It was an arrest that would not have been made, if not for the capability upgrade.

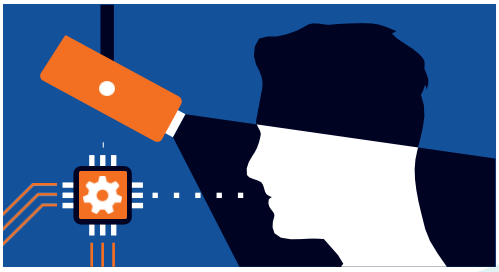
12 http://uk.nec.com/en_GB/press/201707/global_20170711_01.html

STOPPING THE LONE WOLF

Finding a lone wolf attacker early is not always easy. Counter-terrorism officers have to comb through many leads, often going through many false positives. With the help of evolving safer city technologies, they have a better chance of stopping an attack. Here is a list of five SMART steps.

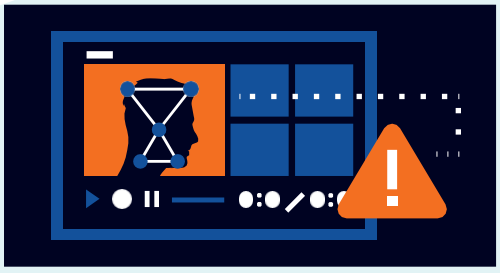
1. Sensing

Analysis of online chatter and browsing patterns help identify a few individuals who often participate in inflammatory rhetoric on a social media network. They may issue threats against a city as well. Meanwhile, the face recognition system at the airport alerts the authorities to one person from the same group who has recently returned from a foreign battlefield. The individuals are placed on a watch list.



2. Monitoring

Through continuous vetting, the AI engine reveals that one member of the group is employed as a security guard at an office tower in the city center. With a license to buy firearms, he tries to purchase a dozen semi-automatic rifles at a gun shop, which alerts the authorities to the large purchase despite everything seemingly checking out. With the facts on hand, the AI virtual agent senses a possible plot and pieces the puzzle together for investigators.



3. Assess

When the group turns up at the building a week later, CCTV surveillance assisted by face recognition quickly picks them up from a database of people to watch out for. The authorities are alerted once again by AI when they are seen circling in a stolen van (checked via license plate recognition) and loitering around a government building.

4. React

To prevent a possible attack, police officers proactively approach the group. They are detained on the spot by police guided to their location. Knives are recovered from them. The authorities foil a potentially deadly plot.

5. Target

One of the group, however, has escaped scrutiny and pulls a knife out on a street full of people. As CCTV cameras capture the panic of people running away, and with updates from the public sent over the mobile network, the authorities are alerted to the unexpected incident. Due to the fast reaction of officers nearby, they rush in and apprehend the suspect swiftly.

PREDICTING AND PREVENTING, NOT PRE-JUDGING

As surveillance becomes commonplace in cities, citizens are also more aware of its reach and scale. One concern is prejudice against groups of citizens, because of the possible profiling and stereotyping that may emerge as part of counter-terrorism efforts.

Security agencies have to guard against pre-judging a case, especially with the additional tools at hand that give them more information and intelligence. What they must focus on are predicting and preventing an incident from happening.

For example, security cameras placed around a city can help analyze behavior and inform law enforcement agencies which areas might require more police presence. This enables a more efficient deployment of officers to deter crime at possible "hot" spots.

AI may be able to spot a dangerous trend, say, a spike in online chatter among persons on a watchlist. Or they may be spotted loitering at a high-profile location. However, the decision to carry out a raid, potentially disrupting an attack, will still have to be based on established standards in evidence collection and after careful investigation.

AI can assist in this. With intelligent prediction, it would take a combination of factors, such as a suspect's travel history or known sympathies for terrorist groups, into consideration before placing him on a watchlist. Instead of profiling a large group of people, this could enable investigators to zoom in on the real suspects plotting to commit a violent crime.

Safety, security and privacy are all important considerations and they are not mutually exclusive. It is important to design and deploy systems that will continue to respect the privacy of the individual while enhancing safety and security.

The need for clear rules of engagement and workflow for authorization of access to data are key elements in systems that support inter-agency collaboration.

An example of this are the standards established in the Fast Identity for Online (FIDO) Alliance. FIDO establishes how biometrics can be effectively utilized to effect online transactions while safeguarding the rights and privacy of the individual.

Chapter 7

NEC SOLUTIONS CAN HELP

At NEC, we have the solutions to help create a better, safer city. We have decades of experience working with governments, city planners and other public agencies in projects as varied as identification to public transport.

Besides the protection of critical installations and safeguarding of cyber infrastructure, our solutions include national identification, law enforcement, immigration, and emergency and disaster response.

Around the world, NEC has worked with governments to build national digital records for citizens to enable free and fair elections and reduce fraud. We helped build the first biometric systems in airports to enable travelers to go through immigration control safely, securely and conveniently.

AI is in our focus in the years ahead. In 2015, NEC announced plans to double the workforce focused on AI to about 1,000. Besides boosting research, NEC is also aiming to double AI-related sales by fiscal 2020.

While bringing together the latest cutting-edge technology, NEC's team also possesses the experience and expertise to deal with projects – both private and government – on municipal and international levels.

In December 2012, NEC signed a three-year-agreement with Interpol to develop core elements of the Digital Crime Centre established at the Interpol Global Complex in Singapore. NEC has provided technical and human resources worth some EUR 7.6 million to set up the Digital Forensic and Cyber-Fusion Centre at the Interpol complex.

This lab focuses on identifying and test-bedding digital forensic technology and methodologies to help investigators better coordinate and conduct digital crime investigations.

Among the cutting-edge technologies is NEC's Cyber Fusion platform. This powerful platform works in tandem with NEC's City Operations Centre, enabling city authorities to tactically tap on connected devices and sensors throughout a city to solicit the necessary signals, for example, to locate suspects of a terrorist attack.

Another important counter-terrorism technology deployed today is NEC's Citizen Collaboration for Security. It empowers citizens to become active participants in improving the city security. They can request emergency services or report events such as accidents or situations requiring response from the city.

This platform is able to receive alerts not only from the dedicated anti-panic devices, but also from other channels, such as mobile applications, POS terminals, SMS and social media networks.

Key to the efforts is a trusted face recognition system. NEC's NeoFace is the gold standard, recognized as the fastest and most accurate algorithm in the world by the National Institute of Standards and Technology in the US. It identifies persons of interest who may be on a watchlist.

Piecing these technologies is together is NEC's AI technologies called NEC the Wise. From face recognition to crowd behavior detection, it monitors a situation in real time, bringing instant attention to an anomaly for quick action.

REFERENCES

1. **London attack as it happened:**
http://www.independent.co.uk/news/uk/home-news/london-attack-live-updates-news-bridge-terror-borough-market-stabbing-van-victims-jihadi-killed-a7772851.html

2. **The London attack is the new face of terrorism — and it's very hard to stop**
https://www.vox.com/world/2017/6/5/15739168/london-attack-terrorism-counter terrorism

3. **ISIS has no air force, but it has an army of drones that drop explosives:**
http://www.newsweek.com/isis-air-force-army-drones-drop-bombs-585331

4. **The myth of the 'lone wolf' terrorist:**
https://www.theguardian.com/news/2017/mar/30/myth-lone-wolf-terrorist

5. **Las Vegas shooter bought 33 guns in last 12 months:**
https://www.usatoday.com/story/news/nation/2017/10/04/las-vegas-shooter-bought-33-guns-last-12-months/730634001/

6. **How UK police are turning to Israel for help stopping 'lone wolf' terror attacks:**
http://www.independent.co.uk/news/world/middle-east/uk-anti-terror-israel-lone-wolf-attacks-help-islamists-advise-westminster-palestinians-london-bridge-a7817286.html

7. **Slipped through net again: London Bridge attacker filmed on Channel 4 unfurling ISIS flag:**
http://www.express.co.uk/news/uk/813075/london-bridge-terror-attack-identity-attacker-ISIS-channel-4-documentary

8. **Pulse nightclub attack: Questions over how suspect on FBI's radar could buy guns:**
https://www.theguardian.com/us-news/2016/jun/13/orlando-nightclub-massacre-suspect-fbi-guns-buy

9. **The 45 recommendations of Lindt cafe siege inquest:**
http://www.smh.com.au/nsw/the-45-recommendations-of-lindt-cafe-siege-inquest-20170524-gwc00o.html

10. **Miyoshi combines efforts with NEC Asia Pacific to market cutting-edge face recognition surveillance product in Asia Pacific:**
http://sg.nec.com/en_SG/press/201708/20170815_01.html

11. **At O'Hare, some passengers undergo face scans in test of security program:**
http://www.chicagotribune.com/news/local/breaking/ct-face-scans-ohare-0720-20170719-story.html

12. **NEC provides facial recognition system to South Wales Police in the UK:**
http://uk.nec.com/en_GB/press/201707/global_20170711_01.html

\Orchestrating a brighter world NEC

WE MAKE CITIES SAFER
Using technologies to safeguard lives and property

Global Safety Division | Transportation and City Infrastructure Division
nec.com/safety safety@gsd.jp.nec.com