A 'Systemic Approach' for Countering the Threat to Public Safety from Improvised Explosive Devices

Chris. W. Johnson, DPhil and Louisa Nilsen-Nygaard;
Dept of Computing Science, Univ. of Glasgow, Scotland, UK.

Keywords: public safety; evacuation; security; counter terrorism

Abstract

This paper argues that a 'systemic' approach can help to address the threat to public safety from Improvised Explosive Devices (IEDs). Rather than focusing narrowly on electronic counter-measures or on the detection of disaffected groups before an incident, we have argued that security agencies should look across all stages of the IED trajectory. We, therefore, enumerate different phases from the preparation of a device through to deployment, execution and the dissemination of propaganda following an attack. These phases are then used to structure an analysis of previous incidents, borrowing a 'lessons learned' approach from more conventional areas of safety-engineering. The intention is that such an analysis can inform scenarios in training tools for security services and for emergency personnel. A secondary aim of our analysis is to identify patterns of attack. These represent tactics that might in the future be transferred between conflict zones in different parts of the world. A key issue in all of this work has been to address the 'failure of imagination' that was criticized by the 9/11 Commission and by subsequent investigations into the London bombings.

Introduction

Improvised Explosive Devices (IEDs) have caused approximately 60% of all American combat casualties in Iraq. In Afghanistan, they have been responsible for 50% of US combat casualties (Ref. 1) and the number of roadside bomb attacks has more than doubled to more than 2,000 in 2008. IEDs remain a weapon of choice not only for attacking military and civil targets but also for making political statements and for attracting media attention. In consequence, the US DoD and Congress have provided $11.25 billion to fund counter-IED programmes between 2004 and 2007. These initiatives have been coordinated by the Joint IED Task Force (JIEDDO) which received $4.35 billion in 2007 alone. The UK Centre for the Protection of National Infrastructure and the US Department of Homeland Security's (DHS) Critical Infrastructure Programme have also focused on increasing the resilience of civil society against IED attacks. In May 2008, the DHS allocated $3billion to secure US critical infrastructure and transportation systems "to prioritize IED prevention and protection, communications capabilities, information sharing, and regionally based security cooperation" (Ref. 2). The extent of this expenditure reflects the importance of IEDs for public safety.

A Systems Safety Approach to Counter IED Operations: IEDs pose a significant threat to public safety around the globe. Many components, especially microelectronics, are easily obtained. At the same time, informal information exchange networks have developed partly based around the Internet that cannot easily be suppressed by security agencies. The exchange of instruction manuals as well as operational feedback, including videos of successful attacks, helps terrorist organizations to rapidly evolve their tactics in the face of strategic and technological countermeasures. Organizations such as JIEDDO have, therefore, begun to pioneer a more 'systemic' approach to counter terrorism. Traditionally, counter terrorism initiatives have been based on relatively narrow security considerations, for example by focusing on the detection of disaffected groups and by the development of specific technical counter measures. Unfortunately, technological countermeasures offer limited protection. For instance, the development of jamming devices has led to the increased use of suicide bombers and to the use of decoy devices in multiple coordinated attacks. Similarly, few security services would be complacent enough to believe that they will always be able to detect or disrupt terrorist groups before an attack can take place. There is now an increasing recognition that we cannot address individual aspects of the problem in isolation – hence detection and disruption of devices must be supported by initiatives to mitigate the consequences of successful attacks.

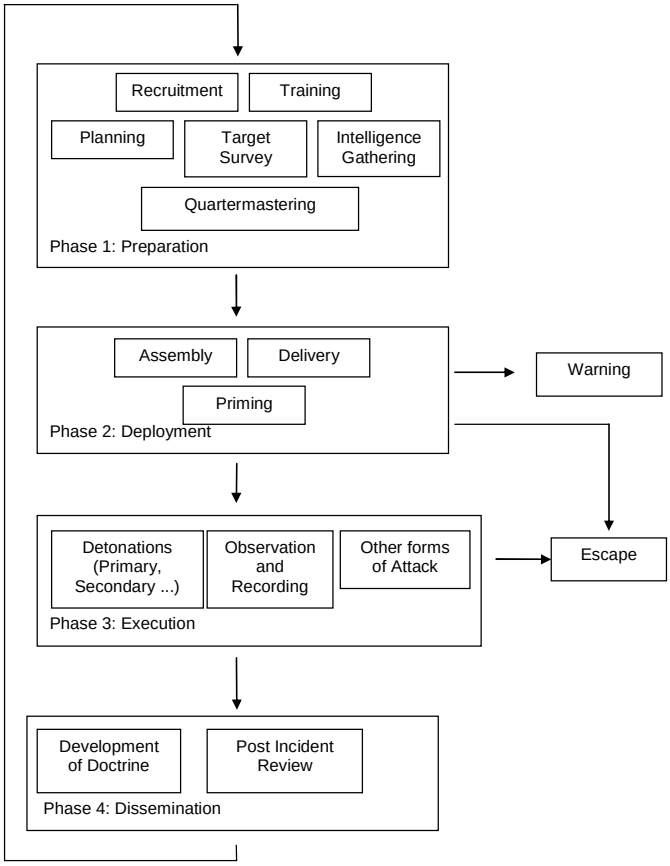

Figure 1: An IED Development Trajectory

In order for such integrated approaches to be successful, it is critical that we learn as much as possible from the ways in which IEDs have been used in previous attacks. By identifying common patterns, it is possible to develop scenarios that can be used in planning for the detection, disruption and mitigation of future attacks. Figure 1 illustrates different aspects or stages of an IED attack. Patterns of attack can be formed by the analysis of each of these stages. As can be seen, the trajectory shown in Figure 1 is a cycle in which the dissemination and publication of reports about 'successful' detonations may help to recruit further attackers. Within each of the phases from preparation through deployment to execution and dissemination, there are more detailed activities that can occur in parallel or in any number of different sequences. For example, the detonation of a primary device may only be part of an attack strategy to catch members of the public in secondary explosions or, as in Mumbai, the detonation of an IED may be part of a wider assault using a variety of different weapons. As mentioned above, much attention has focused on the first and second phase of the trajectory by trying to detect recruitment activities or by training to deploy technological countermeasures immediately after the delivery and priming of a device. However, a key argument in this paper is that systemic approaches to counter-IED programmes should take a far broader view given the relative difficulty of preventing recruitment and the limited success in the deployment of electronic countermeasures in many areas of conflict.

The retrospective analysis of previous IED incidents can only ever form one part of a more integrated approach to public safety. In order to anticipate future attacks, it is important that we can identify and explore a range of future scenarios that help us to avoid the sense of surprise and 'failure of imagination' that was referred to in both the reports of the 9/11 Commission (Ref. 3) and the Intelligence and Security Committee investigation into the London bombings (Ref. 4). Figure 2 presents the interface to computer simulations that have been developed to identify what could happen if IED tactics were transferred from Iraq or Afghanistan to attack the civil population in Europe

or North America. This particular example is based on the busiest railway station in the UK outside of London, with peak weekday occupancy of more than 15,000 people. In this instance, suicide bombers can be identified by the circles that represent the potential targets that would be caught in any blast. The number of people who might be injured changes for each bomber as they and the other passengers move throughout the station concourse in real-time. The size of the blast and fragmentation areas can be varied to allow for larger and smaller devices given the type of explosive used. Each year a table top exercise is held. This involves around 60 staff from the station, transport police and the train operating companies. The exercise is designed to prepare for possible attacks and to help refine the procedures in place for dealing with them. The intention is that this tool can be used by staff to support these annual exercises, for instance, by working through the inter-agency response to a range of different scenarios.

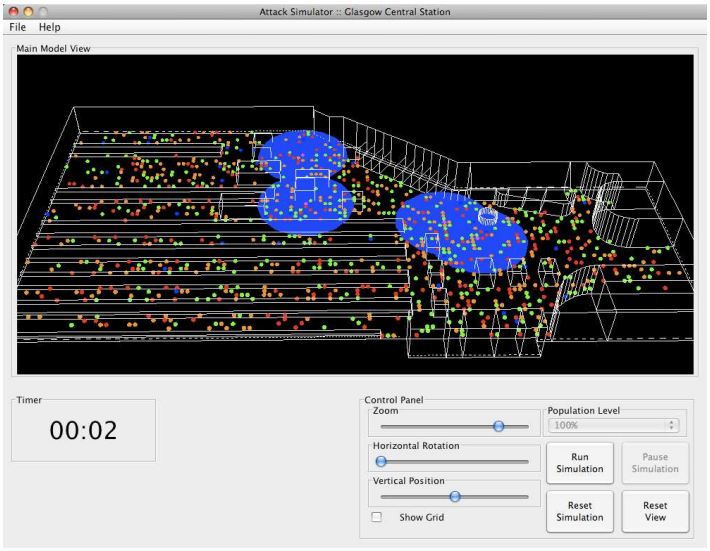

Figure 2: Interface to an IED Simulation

An important aim behind the use of these simulations is to increase civil resilience to future attacks by helping security agencies apply insights gained from previous IED incidents. In order to do this, it is important to learn as much as possible from the large number of attacks that have occurred in different parts of the world. For instance, the scenario shown in Figure 2 is based on two previous incidents. The first involved a suicide attack on Mustansiriyah University in Iraq during January 2007. A car bomb was detonated at one of the two entrances to the site. This led to a partial evacuation that drew crowds to the other exit where a suicide bomber detonated a secondary device. This is not an isolated incident. Hours before, a second coordinated attack took place in a second hand motorcycle market in the Shia Bab al-Sheik neighborhood of Baghdad. The first blast drew onlookers and the emergency services, who were then hit by a second explosion moments later.

Challenge 1: The Global Nature of the Problem

A number of problems frustrate attempts to gather information about IED attacks. There are obvious logistic challenges. For instance, it is possible to obtain a post incident report into the January 2009 suicide car bomb that set fire to a tanker in Kabul; killing four civilians and an American soldier. One reason for this is that it occurred close to a US base and the German embassy. Far less is known about a similar attack that occurred only days later when a civilian died and six people were injured in Nangarhar province. The operational constraints of 'insurgent' areas make it far more difficult to conduct detailed investigations, especially in areas outside the Afghan capital. Further problems stem from the number of blasts that occur around the globe. At almost the same time as the two Afghan blasts mentioned above, an African Union peacekeeper was killed and another injured by a roadside bomb in Mogadishu, Somalia. Less information is known about the tactics and technology used in this incident because African Union forces lack the resources to conduct the same level of examination as the US military. The global

nature of the problem can be illustrated by a series of attacks that all took place in February 2008. For example, anti-government Thai militants killed one person with a bomb buried in a roadway. Four people were wounded. In the same month, an IED killed twenty people and injured eighty more at a bus stop in Sri Lanka. A police officer was killed by an IED close to the Venezuelan Chamber of Commerce in Caracas. On February 8th 2008, two members of the Indian security forces were killed and several others wounded by an IED. There were more than ten IED attacks in India alone within a four week period earlier this year. The frequency of these incidents, together with the geographical distribution frustrates attempts to create an international database similar to those that are used to collate 'lessons learned' across the aviation safety community. There are profound differences in the quality of information that is available to intelligence agencies following IED attacks. In consequence, we must gradually identify common patterns that reflect changing tactics and technologies from partial accounts of a subset of all the IED attacks that occur across a wide range of conflicts.

Challenge 2: Simulating Different Designs for IEDs

Simulators, such as the system illustrated in Figure 2, can help security services train for the impact of an IED attack. One of the difficulties in developing these tools is the diversity of different devices that have been used; these range from the pipe bombs that target specific individuals up to vehicle-based devices that destroy entire districts. It can also be difficult to develop simulations that account for innovations in IED technology. For example, many of the weapons used in Iraq are simple platter charges. These are constructed from several kilograms of plastic explosive pressed into a similar mass of flat metal, typically steel. This will propel the platter into a target with an approximate velocity of 1,800 m/s at up to 50m. For other targets, Explosively Formed Penetrators (EFPs) have been deployed. In these devices, the force of a blast helps to form a penetrating projectile that can be effective more than 80m from the target. Cylindrical shaped charges can be tipped with a concave metal disc, typically made of copper. Variants on this type of device have been successfully deployed against Abrams M1A2 tanks. US Army field manual FM20-32 provides a useful starting point for the development of counter terrorism simulators because it provides an initial taxonomy for improvised explosive devices. It distinguishes between high-explosive, artillery-shell antitank devices, platter charges, improvised Claymores, grapeshot antipersonnel devices and barbwire antipersonnel devices. FM20-32 focuses on devices that have been used against organized military units. All of these IEDs have also been used on civil populations in different parts of the globe.

Challenge 3: Assessing the Quality of Explosives

The power of an IED can be measured in terms of the blast and fragmentation that it produces. These parameters are partially determined by the quantity or quality of explosive. In some areas, terrorist and insurgent groups must improvise 'home brew' explosives from off the shelf ingredients. However, many devices have been constructed from military munitions that have been stolen from supply lines. For instance, Chinese and North Koreans forces massively underestimated their need for mines in response to the defensive tactics used by UN forces during the Korean War. They, therefore, improvised a series of 'battlefield devices' many of which relied upon mines that had been lifted from UN positions. The same techniques were also widely employed by the Viet Cong during the Vietnam conflict (Ref. 5). 33% of U.S. casualties in Vietnam were caused by mines including IEDs that used trip wires and rubber bands to detonate grenades (Ref. 6). The reuse of munitions in IEDs illustrates the 'systemic nature' of the problem. Rather than focus narrowly on technological countermeasures once a device has been planted, more may be gained by securing supply lines. This point was recognized in a recent report by the US Government Accountability Office. They argued that the DoD planning for Operation Iraqi Freedom had incorrectly assumed the Iraqi army would rapidly be convinced to provide security for their stockpiles of conventional munitions once they had surrendered. In consequence, a large number of conventional munitions were 'looted'. These munitions were subsequently used in the majority of IEDs deployed against allied forces. The GAO concluded that "…DOD's actions generally have emphasized countering the use of IEDs by resistance groups during post-hostility operations… GAO also concludes that this situation shows both that Iraqi stockpiles of munitions may not be an anomaly and that information on the amount and location of an adversary's munitions can represent a strategic planning consideration for future operations. However, without joint guidance, DOD cannot ensure that Operation Iraqi Freedom lessons learned about the security of an adversary's conventional munitions storage sites will be integrated into future operations planning and execution" (Ref. 7). This provides a direct illustration of the impact that 'systems safety' thinking has had upon recent counter-IED programs.

Challenge 4: Planning for Large Scale Attacks

In developing simulation tools to help security forces anticipate the impact of IED attacks in Europe and North America, it is less likely that terrorists would have access to military grade explosives. However, there is little room for complacency. TNT and the C4 compound were used in the 2008 attack on the Islamabad Marriot. More than a ton of fertilizer-based explosive was used in the 1992 IRA attack on the Baltic Exchange building in the City of London. This killed 3 people and caused £350 million of damage. A similar quantity of 'home brew' compound was used in the 1993 attack on Bishopsgate in the same City, injuring 40 people and caused damage totaling more than £1 billion. This IED was hidden in a construction truck and left a crater more than 40ft wide and 20ft deep. A half ton bomb under South Quay station caused £85 million of damage to London's Docklands in February 1996. A ton and a half of improvised explosive was used in a failed attempt to destroy Canary Wharf tower in November 1992, but the detonator failed to ignite the main charge. A slightly larger lorry-based IED injured more than 200 people in Manchester city centre in June 1996. This remains the largest bomb to explode in the UK since the Second World War and was parked under a shopping center some two hours before detonation. It was subsequently estimated that up to 50,000 square meters of retail space and nearly 25,000 square meters of office space had to be reconstructed. Similar tactics have been repeated across the globe. Three quarters of a ton of a fertilizer-based compound was detonated in the underground car park at the World Trade Centre in 1993. A more destructive form of 'home brew' explosive was used in the Oklahoma City bombing. The ease with which the two conspirators were able to amass more than 2,300 kg of explosive-grade ammonium nitrate fertilizer and 600 liters of liquid nitromethane is an instructive lesson for security agencies around the globe. Similar compounds were used in the Bali bombings of 2002 that killed more than 200 people and in multiple attacks on US embassies in August 1998 killing 224 people. One of the key insights from this enumeration is the continuing vulnerability of civil society to these weapons. The insights derived from the consulate bombings of the 1990s still did not yield enough counter measures to prevent the 2002 attack on the US embassy in Karachi where a truck based fertilizer bomb killed 12 and injured 51. Even when we are forewarned about the types of target involved, IEDs have been successfully used by increasing the force of the device or by changing tactics, for example from delay based detonators to suicide attacks. The Al Qaida attack on the British Consulate in Istanbul and the HSBC bank killed 30 people even though security personnel were aware that they might have been at some risk; suicide bombers detonated a mixture of ammonium nitrate and fuel oil in pick-up trucks. Simulators can help planners to consider a wider range of attack scenarios, for example by considering 'what if' tactics were exported from Iraq or Afghanistan to Europe or North America. However, it is equally important not to forget the lessons provided by the large scale vehicle-based devices from the 1990s. An effective way of focusing the attention of building owners and occupiers is to show them what might happen if they were attacked using the size of devices that were deployed against Bishopgate or the Federal Buildings in Oklahoma. It can be far more convincing to develop training scenarios where the impact of the IED is based on a device that has already been detonated in London or New York rather than Baghdad or Beirut.

Challenge 5: Planning for Medium Scale Attacks

Large scale devices usually require quartermasters to coordinate the acquisition and storage of materials before an IED can be assembled. There are often, therefore, opportunities for security forces to detect the build-up of components. This is another reason why it is so important to study the ways in which the perpetrators of previous attacks were able to acquire their materials. In contrast, medium scale IEDs are far harder to detect because they can be improvised from limited quantities of legitimate components with very little prior planning. The unpredictable nature of these attacks can be illustrated by recent attempts to detonate IEDs in London and at Glasgow Airport. The initial plan was to load two cars with gas canisters on the back seats; together with nails and petrol in the trunk. Mobile phones had been rigged to provide improvised detonators. The cars were driven from Scotland to London in June 2008. The first vehicle was parked outside a nightclub. The second was parked a few streets away; with the possible intention of catching people in a secondary blast. This plot clearly differs in scale and the sophistication of the explosives from those described in previous paragraphs. It also illustrates that any narrow attempts to identify potential attacks from the purchase of ammonium nitrate may underestimate human ingenuity. This initial plot failed when 15 calls to the mobile phones failed to trigger the detonation. The attackers then returned to Scotland and rigged up a third vehicle with fuel and gas canisters, petrol and knives. Rather than leaving the vehicle outside a night club, the attackers drove it into the main doors of Glasgow airport where it was wedged against a steel block. This device also failed to detonate, possibly due to the difficulty of ensuring that the mixture of fuel and oxygen fell

within the flammable range. The attack on Glasgow Airport provides a further motivation for studying previous IED attacks to inform safety campaigns. Prior to this attack, there was arguably a sense of complacency in Scotland. Public and politicians felt there was little risk that we would be the target for a terrorist attack. IEDs were associated with conflicts on the other side of the globe. This attitude faded as soon as the vehicle was driven into the airport. The simulation tool, illustrated in Figure 2, was explicitly developed as part of a wider programme to increase the resilience of Scots infrastructure against the future threat posed by these devices.

Challenge 6: Planning for Attacks against Individuals

In contrast to the enormous devices used in Bishopgate or the Federal buildings in Oklahoma City, some IEDs are specifically intended to kill or injure individuals. An example is provided by the pipe bomb that injured Zeev Sternhell, an Israeli academic and critic of Jewish settlement in the occupied West Bank. Car bombs have also been widely used in many countries, for instance a mercury tilt switch was used to detonate the device that killed Airy Neave, a UK Conservative politician who was known to take a hard line against loyalist and republican paramilitaries. Similar devices were used to target individuals who had been opposed to the regime of Augusto Pinochet in Chile. Mail bombs have a history that is almost as long as the postal service; they are 18th century accounts from both Italy and Denmark. The Unabomber provides more recent examples. His first device was found in a parking lot. The return address was that of the intended victim. The parcel was eventually passed to a security guard who received minor injuries when he attempted to open it. The first devices were relatively crude pipe bombs with wooden end pieces and detonators that pulled a nail across match heads. Later devices replaced this approach with batteries and filament wire, including an IED that was placed in the hold of an aircraft flying within the United States. In the UK, mail bombs have recently been sent to companies involved in DNA testing. A primary school caretaker was eventually arrested and subsequently argued that the small amount of explosives was intended to increase public awareness without causing injury. These arguments were largely dismissed by the court. In the US, a series of unassembled letter bombs were sent by someone calling themselves 'The Bishop' to financial firms in the Midwestern United States. Subsequent investigations have suggested that the individual involved was copying elements of a Charles Bronson film in which an assassin left a note with each bomb. Considerable care had to be taken during the arrest of 'The Bishop'; as in similar cases there was concern that they might detonate a device during the arrest. Crowd based modeling tools, such as that shown in Figure 2, help planning and training for these police actions. The fatal shooting of Jean Charles de Menezes by UK police shows other 'systemic' aspects of IED attacks that can be addressed through the use of modeling tools. This Brazilian electrician was mistaken for a suicide bomber with links to the 21st July attacks on London. The subsequent inquest showed that security services must revise the way in which they plan for the arrest of terrorist suspects. This can be done through the use of simulations that recreate the flow of information between intelligence services; including the problems in information exchange that characterize real world operations rather than the ideal situation often portrayed in Standard Operating Procedures. One of the problems for security services is that the same level of care must often be taken with individuals who may not ultimately be shown to pose a significant threat to public safety. This creates problems because subsequent proceedings can undermine the credibility of counter terrorism work. An example is provided by the prosecution of a man who was found not guilty in the UK of two charges of making IEDs. During the trial it emerged that army disposal experts found fireworks and 'thunderflash devices' in his home. They also found an infrared transmitter that was capable of triggering the detonation of an IED. However, the defense successfully argued that this was used to operate his satellite television and that the defendant had an interest in fireworks from teenage years. In stark contrast, the increasing use of IEDs can also be illustrated by a successful UK prosecution of a man who was found to be in possession of a nail bomb when bailiffs came to evict him from his house. The army bomb-disposal teams again had to make the device safe before neighbors could return to their homes.

Challenge 7: Delivery Mechanisms

Figure 1 presented a trajectory for IED attacks; this is intended to structure a more systemic view of the threats presented by these devices. As can be seen, a key element of the second phase is the delivery of an IED to its intended target. In some cases, this can seem like an elaborate term for a relatively simple act. For example, thirteen people were injured in November 2008 when an IED was thrown from a flyover into a market in Bangkok. This incident illustrates the diverse nature of the threat from these devices; the incident was not part of an ethnic or political dispute but seems to have been a response to a civil dispute between traders and the market management

following a rent increase. Previous sections have already summarized several other delivery techniques ranging from cars, vans and trucks through to the postal systems that convey letter and parcel bombs. The diversity of delivery mechanisms challenges some of the 'silo thinking' that characterizes the immediate response to IEDs in many countries. For instance, many airports, railway stations and shopping malls have responded to attacks such as the one at Glasgow Airport by pouring vast quantities of concrete to prevent the use of car bombs. At the same time, these facilities are encouraging the use of 'greener forms' of transport including bikes, they are increasing accessibility to individuals in wheelchairs and to families using child buggies. All of these different forms of 'transport' have recently been used to deliver IEDs. For instance, one person was killed and four people were wounded by an IED that was detonated in India during February 2008. Several of these improvised devices created many times the blast and fragmentation than could have been produced by the materials in the four by four that was used to ram the airport buildings. A key distinction between many of these delivery mechanisms is whether or not the perpetrators intend to carry out a suicide attack. Figure 1 shows this in the trajectory model through several different stages at which perpetrators might attempt to escape detention. Vehicle based bombs with delayed detonation, such as those used by the IRA against the City of London, can be contrasted with a host of more recent suicide attacks such as three recent blasts in Algeria; attributed to the Islamist insurgency. A car containing an IED was driven into a police college in Issers, killing almost 50 recruits waiting for an exam. Within twenty-four hours another two car bombs were detonated near a barracks in Bouira. Suicide bombs have been used in countries as diverse as Turkey, where 6 people were killed and 90 injured in Ankara in May 2007, and Pakistan, where the2008 attack on the Marriott Hotel in Islamabad killed more than 50 people and injured more than 200. In Vladikavkaz, the capital of the North Ossetia region between Russia and Georgia, eight people were killed in November 2008 by a female suicide bomber outside a busy market. The device was detonated as a minibus arrived at a bus stop. Numerous other examples can be cited from the conflict with Chechnya. In contrast to these relatively primitive delivery mechanisms, it is likely that the transfer of IED design techniques will continue to influence future delivery mechanisms – for instance, through the development of rocket based devices similar to those being fired into Israel. Hezbollah have used Katyushas from former Soviet and Chinese stockpiles, such as the Soviet BM-21 Grad missile as well as 'derivatives' from the Iranian Fajr missiles. These delivery systems are not considered in detail in this report because they are closer to standard military munitions than the majority of 'improvised' explosive devices.

Challenge 8: The Dynamic Refinement of IED Technology and the IED 'Arms Race'

A further challenge in developing the scenarios that can be used to train for future IED attacks is that the technologies used by terrorists and insurgents change over time. In other words, we should never underestimate the role of improvisation in the development of these devices. This can be illustrated by recent blasts in which IEDs were hidden inside ATMs, or cash machines, although these were not programmed to recognize individual PIN numbers. The evolution of new techniques emphasizes the need both to learn and extrapolate from previous attacks around the globe. The gradual increase in the sophistication of IEDs can be seen in the development of technology used during the Northern Ireland 'Troubles'. These ranged from Molotov cocktails through to remotely controlled devices with anti-handling features, such as tilt switches, that would detonate if attempts were made to defuse or move the IED. Many of the techniques had been used in previous conflicts, such as clockwork timers with five to ten minutes delay. However, the Brighton Hotel Bomb was planted more than twenty days prior to its detonation. This device was constructed using the timer components from VHS video recorders. Other 'innovative' devices were constructed using transceivers and servo motors from model aircraft. Technical innovation did not cease with the Mitchell peace process. Previous generations of pressure pad detonators have been replaced by infrared triggers. IED's have also been developed to exploit GSM and other forms of radio signals, including pulsed transmissions that can offer greater resilience to jamming. Security forces have responded by installing electronic counter measures such as the 'Element B' systems. However, these innovations seldom offer complete protection. They can be difficult to install and maintain across all of the vehicles used in many conflict areas. They can also create tensions when, for example, allied troops are protected while the same counter measures are not available to local coalition forces. The IED 'arms race' continues not only in the iterative improvement of remote detonation but also in the use of Explosively Formed Penetrators (EFPs) to counteract changes in vehicle protection. The systems approach, advocated in this paper, stresses that there innovations cannot be considered in isolation from the many tactical changes that have profoundly changed the ways in which IEDs are deployed in recent months.

Challenge 9: The Dynamic Refinement of IED Tactics

Many of the tactics used in recent IED attacks were first developed by Hezbollah following Israel's invasion into Lebanon. In the mid 1980s, suicide bombers were used to drive vehicles against their intended targets. However, security forces changed their tactics to reduce the opportunities for this form of attack. Physical barriers were used to segregate civil traffic from potential targets. In consequence, greater emphasis was placed on the use of roadside bombs planted well in advance of their detonation. This tactic was used in the remotely detonated bomb that killed Israeli Brigadier General Erez Gerstein in February 1999. Since that time, the Israeli's have continued to pioneer IED countermeasures. However, they recognize that there can never be complete protection from this form of attack. The building of the Gaza wall illustrates the difficulty of preventing IEDs. Western security forces have copied many of the counter measures adopted by the Israelis, for instance in segregating potential bombers from their targets. However, there are strong suspicions that members of Hezbollah, assisted by Iranian Revolutionary Guards, helped to transfer expertise in the use of IEDs to the local militias that attacked British forces around Basra. These suspicions are supported by the transfer of specific techniques between these conflicts. For instance, Hezbollah developed the use of stacked mines to increase the blast that was needed to destroy Israeli vehicles. The same approach has been used against US forces in Western Iraq during 2005. There are other parallels in the tactics used to conceal roadside bombs as false rocks and road-kill in Lebanon and in Afghanistan. Explosively Formed Penetrators or 'shaped charges' have also been used in all three conflicts. One of the catalysts for the exchange of IED tactics has been video footage of the attacks. Hezbollah quickly recognized the propaganda impact of filming their work. This raised awareness of their operations and may also have helped recruit additional support. However, the videos had further uses; they were included in training manuals and were studied to improve subsequent tactics. These developments reiterate the importance of 'systemic approaches' to IEDs. Not only must security agencies focus on countermeasures and the detection of present threats, they must also consider the impact that such documentation and video footage can have upon the shape of future threats. In particular, a detailed analysis of Internet video footage might provide scenarios for simulations, such as that shown in Figure 2, so that the study of previous attacks can inform the training of security personnel just as it presently informs the training of future bombers.

Challenge 10: Multiple Coordinated Attacks

Previous sections have described the increasing threat posed by the use of coordinated IEDs. Terrorist and insurgent groups have learned that multiple simultaneous attacks carry a greater impact than a series of isolated detonations. One of the early examples of this was provided by the coordinated attack on US Embassies perpetrated by Al Qaida during August 1998. 224 people were killed by bombings in Nairobi, Kenya, and Dar es Salaam, Tanzania. These attacks illustrate the importance of being able to extrapolate from previous attacks – they are widely recognized as precursors not just of the London and Madrid bombings but also of the 9/11 attacks. It seems unlikely that analysis could easily extrapolate from the embassy explosions to anticipate these subsequent attacks. However, official reports into all these incidents have made the point that it is precisely this 'leap of imagination' that we should encourage in our security services. It is possible to identify other emerging patterns that might provide precursors to future attacks. For example, the opening sections of this paper explained that the simulation tools in Figure 2 were based on the coordinated use of IEDs in Iraq. In several previous incidents, a primary car bomb was detonated before suicide bombers used secondary blasts to target the crowds that gathered after an initial explosion. This pattern can also be seen in the 2002 Bali bombings; a suicide bomber first triggered a backpack device in a bar. The crowds that then fled from the scene of this first blast were caught by a secondary fertilizer-based IED hidden in a van. Further variations on the coordinated use of IEDs have emerged from the Mumbai attacks in December 2008. Ten gunmen fired at a number of points in India's largest city over a 60 hour period. IEDs were not the primary weapons used; however, they did play an important role. Two devices were found in the wreckage of the Taj Mahal Palace hotel – Police have not disclosed the details but they did comment on the relative sophistication of their construction, especially of the timing devices. Following the attacks, security agencies conducted a sweep of Chhatrapati Shivaji train station and declared it to be safe. However, several days later IEDs were found amongst lost luggage. The public again had to be cleared from the building. It is, therefore, possible to identify several different patterns in the coordinate use of IEDs – these include near simultaneous attacks in different countries, simultaneous attacks across the transportation or other infrastructures in the same country, the coordinated use of suicide bombers and vehicle based devices to draw crowds into secondary explosions, the use of armed attacks in conjunction with IEDs that may then be used to target security forces etc. It is clear that most local security agencies in Europe and in North America have only begun to consider a very limited subset of the scenarios that have already been witnessed in other areas of the globe. This has significant and pressing implications for future public safety.

Challenge 11: Delayed Warnings, Hoaxes and the Scope for Intervention

Previous sections have described a series of challenges that complicate the task of developing training tools and simulations that help emergency and security personnel to train for the future threats posed by Improvised Explosive Devices. A key theme in this work has been to use a 'systemic' model covering diverse phases in the preparation of an IED through to deployment, execution and dissemination for different patterns of attack (Ref. 8). Previous sections have not, however, considered the limited opportunities that we have to respond to IED attacks. Technical innovation continues to increase our ability to counteract the masking techniques used to disguise IEDs prior to detonation. However, sensing systems are still limited in their range and by the costs both of installing and maintaining them. They also create significant overheads when security personnel are forced to respond to a large number of 'false hits'. These insights are illustrated by the five million security alerts that were logged during the 16 days of the Turin Winter Games, a figure that was exceeded in Beijing (Ref. 9). The technical issues are further complicated by ethical concerns over the consequences for civil liberties and concerns following incidents such as the fatal shooting of Jean Charles de Menezes, mentioned in previous sections. It seems likely, therefore, that the primary response to a potential IED attack will continue to depend upon input from the public or from the warnings that are often issued by the perpetrators of an attack – either to reduce public casualties or increase injuries sustained by the emergency services. For example, a warning was issued some forty minutes before the Omagh bomb exploded. This was ambiguous and Police began clearing the wrong area. Instead members of the public, including women and children, were directed towards the bomb. It is vital that we learn the lessons provided by these previous incidents. For example, the 911 operator who received the warning about the pipe bomb in Centennial park during the Atlanta Olympic Games could not dispatch a response team because she could not enter 'Centennial' into her computer system; this had not been updated with the new names given to major venues as part of the preparations for the Games (Ref. 10). The operator was eventually put on hold for two minutes while the Command Center began asking for the street address of the Park. In the meantime, members of the public had reported a suspicious bag but officers on the scene were reluctant to broadcast a warning in case panic ensued. Police teams reached the Park just as the device exploded. Just as important as learning the lessons from previous incidents, is the need to inform our future response by studying previous hoax calls. More than 100 reports of suspicious packages were made in the 24 hours following the explosion in Centennial Park. All proved to be harmless but these incidents placed immense stress on the police and other security agencies. The paradoxical effect of increasing public awareness was that the sheer number of false alarms may have created opportunities for subsequent malicious acts. It is important not to underestimate the impact of these calls. For instance, one report led to the closure of the 'Underground Atlanta' shopping mall. Thousands of people had to be evacuated during the evening following the bombing. Although the subsequent search lasted less than an hour, the evacuation caused considerable traffic problems. The mall was adjacent to the Five Points interconnection for Atlanta's MARTA rapid transit system. Thousands more people were affected when this main north-south and east-west transfer point was closed. The package turned out to be a clothes iron.

Conclusions and Further Work

This paper has argued that a 'systemic' approach can help to address the threat to public safety from Improvised Explosive Devices (IEDs). Rather than focusing narrowly on electronic counter-measures or on the detection of disaffected groups before an incident, we have argued that security agencies should look across all stages of the IED trajectory. Figure 1, therefore, enumerated different phases from the preparation of a device through to deployment, execution and the dissemination of propaganda following an attack. These phases were then used to structure an analysis of previous incidents, borrowing a 'lessons learned' approach from safety engineering. The intention is that such an analysis can be used to inform the scenarios that are used in training tools and in incident simulators for security services and for emergency personnel. A secondary aim in this analysis has been to identify patterns of attack. These trends can help to identify future tactics that might be transferred between conflict zones in different parts of the world. It is important not simply to focus on past events but also to use previous lessons as a means of preparing for future attacks. Further work, therefore, intends to develop more systematic techniques to transfer these previous lessons into scenario development using dynamic Bayesian techniques, including hidden Markov models. A key issue in all of this work has been to address the 'failure of imagination' that was criticized in the report of the 9/11 Commission and by subsequent investigations into the London bombings.

Acknowledgements

We are extremely grateful to the three reviewers who provided valuable advice and who helped to guide the final draft of this paper. All remaining errors and omissions remain the responsibility of the authors.

References

1. Congressional Research Service, Improvised Explosive Devices (IEDs) in Iraq and Afghanistan: Effects and Countermeasures (Washington, D.C.: Aug. 28, 2007).
2. Department of Homeland Security, DHS Awards $844 Million to Secure Nation's Critical Infrastructure, May 16, 2008, Washington D.C., USA. Available from http://www.dhs.gov.
3. 9/11 Commission, Report of the 9/11 Commission, Washington D.C., USA. Available from http://www.9-11commission.gov/report/911Report.pdf
4. Intelligence and Security Committee Report into the London Terrorist Attacks on 7 July 2005, Report Cm 6785, Her Majesty's Stationery Office, Norwich, UK.
5. H.E. Dickenson, Chief of Staff, First Marine Division (Rein), Division Order P3820.2A, Standard Operating Procedures for the First Marine Division: Countermeasures Against Mines and Booby-Traps (San Francisco: Department of the Army Office, Chief of Engineers, February 1, 1969), p. 1-1, as republished in Smith, Landmines/Vietnam (1972), p. H-39.
6. Harry N. Hambric and William C. Schneck, The Antipersonnel Mine Threat: A Historical Perspective, Symposium on Technology and the Mine Problem, Naval Postgraduate School, Monterey, CA, November 18-22, 1996, p. 15.
7. Operation Iraqi Freedom: DOD Should Apply Lessons Learned Concerning the Need for Security over Conventional Munitions Storage Sites to Future Operations Planning, GAO-07-444 March 22, 2007, http://www.gao.gov/products/GAO-07-444.
8. C.W. Johnson and L. Nilsen-Nygaard, Extending the Use of Evacuation Simulators to Support Counter-Terrorism: Using Models of Human Behavior to Coordinate Emergency Responses to Improvised Explosive Devices. In R.J. Simmons and D.J. Mohan and M. Mullane (eds), Proceedings of the 26th International Conference on Systems Safety, Vancouver, Canada 2008, International Systems Safety Society, Unionville, VA, USA, 0-9721385-8-7, 2008.
9. C.W. Johnson, On the Convergence of Physical and Digital Security for Public Safety at Olympic Events. In R.J. Simmons and D.J. Mohan and M. Mullane (eds), Proceedings of the 26th International Conference on Systems Safety, Vancouver, Canada 2008, International Systems Safety Society, Unionville, VA, USA, 0-9721385-8-7, 2008.
10. C.W. Johnson, Using Evacuation Simulations to Ensure the Safety and Security of the 2012 Olympic Venues, Safety Science, (46)2:302-322, 2008.

Acknowledgement

This work was produced as part of an EPSRC/BAE Systems CASE studentship. Thanks are due to anonymous reviewers inside BAE who provided valuable feedback on an initial draft of this work.

Biography

Chris.W. Johnson, DPhil, MA, MSc, FBCS, CEng, CITP, Department of Computing Science, University of Glasgow, Glasgow, G12 8RZ, Scotland, UK, telephone +44 (141) 330 6053, facsimile +44 (141) 330 4913, e-mail – Johnson@dcs.gla.ac.uk, web page http://www.dcs.gla.ac.uk/~johnson

Chris Johnson is Professor of Computing Science at the University of Glasgow in Scotland. He heads a small research group devoted to improving the reporting and analysis of incidents and accidents across safety-critical domains ranging from healthcare, to the military to aviation and rail.

Louisa Nilsen-Nygaard, Department of Computing Science, University of Glasgow, Glasgow, G12 8RZ, Scotland, UK, telephone +44 (141) 330 2000 ext 0917, email louisa@dcs.gla.ac.uk, web page http://www.dcs.gla.ac.uk/~louisa

Louisa Nilsen-Nygaard is PhD student in the Computing Science Department at the University of Glasgow in Scotland. Louisa is doing research into using computer simulation to determine counter defences to improvised explosive devices.