JOURNAL OF TERRORISM & CYBER INSURANCE

THE JOURNAL OF TERRORISM & CYBER INSURANCE

www.terrorismcyberinsurance.com

team@terrorismcyberinsurance.com

November 2017

Vol 1 No 4

WELCOME

The team at the Journal of Terrorism & Cyber Insurance are proud to bring you the fourth issue of the Journal of Terrorism and Cyber Insurance.

This fourth edition continues from our earlier editions of the Journal where we featured comments, trends, advice and expert opinions from key global insurance industry professionals, counter terrorism experts and cyber security professionals on the state of the terrorism and cyber insurance market and likely challenges.

We thank you for reading the Journal and hope you enjoy all of the contents, articles and features in this edition.

JTCI ONLINE

We welcome followers and subscribers on all our online presences. We also encourage readers to sign up to our email list (website, right hand column, or email team@terrorismcyberinsurance.com).


team@TerrorismCyberInsurance.com


www.TerrorismCyberInsurance.com


www.terrorismcyberinsurance.com/feeds/posts/default


www.Facebook.com/TerrorismCyberInsurance


ww.Twitter.com/TerrorCyberIns


www.linkedin.com/company/journal-terrorism-cyber-insurance

SPONSORS

We are very thankful for the continued support of our key corporate sponsor, Property Claims Services (PCS, a division of Verisk Analytics).

PCS' Tom Johansmeyer: "The terror threat is shifting. Adaptation and collaboration is necessary to ensure (re)insurance products are fit for purpose and can be employed to deploy capital efficiently when times are tough... The need for greater focus on improved risk and capital management relative to terror and cyber has only gained momentum over the past year, and the trajectory seems likely to continue. The Journal of Terrorism & Cyber Insurance provides a crucial forum for the exchange of thought leadership and commercial insights that can help re/insurers allocate capital more effectively and – more importantly – communities and businesses recover from an event. The role of the insurance industry is to protect the insured and society. The JTCI should provide a forum to help advance that mission."

UK Security Expo – The Global High-End Security Showcase 29-30 November, London Olympia

UK Security Expo is a major-scale event bringing 10,000+ International Visitors to London to tackle some of the most challenging security threats to our citizens, borders and infrastructure. There are over 250 free-to-attend sessions over both days of the show, with topics ranging from Cyber, Global Counter Terrorism, Protecting Crowded Places and Critical National Infrastructure Security.

Find out more at www.uksecurityexpo.com/jcti
Claim a complimentary Visitor Pass now - www.uksecurityexpo.com/jctireg

Table of Contents

Welcome	2
Sponsors	3
In Brief: Commentary From The Industry	7
Terror Public Private Cover	9
Addressing Cyber Cats Through A Parametric Trigger Structure	13
Without Territory What Will The So-Called Islamic State Become?	16
Counterfactual Analysis Of The 2017 Barcelona Terrorist Attack	18
Legal	26

Original Risk

Take a Bite

Tempted by Sustained Profitable Growth?

For more information, please contact:

Tom Johansmeyer
AVP – PCS® Strategy and Development
+1 201 469 3140
tjohansmeyer@iso.com

#originalrisk

verisk.com/originalrisk

PCS

IN BRIEF: COMMENTARY FROM THE INDUSTRY

"The cyber enabled threat is growing. With North Korea now being blamed for the WannaCry attack, who was responsible for the costlier notPetya attack - and are we seeing the beta testing elements of a new era of cyber weapons? One thing is certain: with greater political instability globally, the state enabled cyber threat is growing and enterprise are a key target."

Philip Ingram MBE, Founder Grey Hare Media

"One of the most critical steps in developing cyber models is developing an accurate historical database of large cyber events. The PCS Global Cyber Index will help the industry develop these databases through proper identification and quantification of major cyber events."

Nicholas Irwin, Lead Cyber Actuary.
Verisk Analytics

"As a global society and economy, we are quickly coming to the realization that the key is resilience since we cannot prevent all cyber attacks. The PCS Global Cyber Index pioneers the extension of the risk transfer chain to achieve that economic resilience."

Prashant Pai, Vice President, Cyber Strategy.
Verisk Analytics

A key challenge for cyber risk transfer is data. Historically, data has not been collected in a digital format. Secondly, the insurance industry is often hypothesis focussed. Insuretech is solving both of those problems. Data is now being gathered in a consistent, exploitable fashion at huge volumes. This facilitates a paradigm shift from hypothesis to correlation, removing bias. At Corax we ask "What signal is in the data?," allowing us to separate the important from the merely interesting."

Marcus Breese, Head of Insurance Innovation & Strategy
Corax

"There is a growing move towards addressing the first-party issue in Cyber insurance, as knowledge of how major events can result in significant losses to a business become more widespread. This is particularly seen in the larger corporate space following announcements by global enterprises of the financial impact of WannaCry and NotPetya were made to shareholders, extending into the hundreds of millions of dollars. The trickle-down effect is that smaller businesses are looking to the insurance industry to provide answers, with this being as much about policy coverage as it is risk management support and breach response services. Forward-planning measures such as Business Continuity Planning can need expert input owing to the potential impact of a cyber incident affecting all areas of a business, whilst having contracted access to incident/claims response – including IT forensics, data breach counsel, and Public Relations experts – will make all the difference when the insurance comes to be called upon. Having this in a formalised and holistic package is the best way to avoid troubles later down the line, and the more advanced cyber insurance providers are already offering these services. I chaired HDI Global's cyber workshop at this year's AIRMIC conference in Birmingham, and had representation from insurance, legal, IT security and probably most importantly the insurance purchaser as part of my panel. The purchaser talked through their journey from internal review to risk transfer via quantification of impact and completion of loss scenarios, and from there was able to identify what support they truly needed with a view to finding the best insurer to support their needs both in terms of coverage and the other services mentioned above. Ongoing dialogue between insurers, buyers and their brokers will continue to shape how this area of insurance develops and best serves all parties. Cyber insurance is undoubtedly a specialist market; however this brings the great benefit of truly finessed products being made available as understanding of exposures continues to grow – particularly with buyers and them gaining access to insurance which fits their individual needs."

Peter Hawley, Cyber Underwriter,
HDI Global SE

TERROR PUBLIC PRIVATE COVER
(1.5 minute read)

Background

France offers one of the world's most extensive forms of coverage against acts of terrorism. Since 1986, the date on which specific legislation came into effect, property coverage against attacks and acts of terrorism has been compulsory for both business and personal property insurance policies. This coverage applies mainly to property damage resulting from a terrorist attack or an act of terrorism occurring on national territory. Additionally, bodily damage is covered by a public fund "Fond de Garantie des Victimes des Actes de Terrorismes et d'autres Infractions – FGTI" (Guaranty Fund for the Victims of Terrorism and other Offenses).

Scope and Cover

Under Article L 126-2 of the French Insurance Code (Code des Assurances), it is mandatory for insurance policies covering Property Fire Damage on national territory and damage to land motor vehicles, to cover "…direct material damage to the insured property caused by a terrorist attack or act of terrorism... sustained on national territory."
The scope of the compulsory cover extends to acts of terrorism committed using nuclear, biological, chemical or radiological agents (NBCR). Recoveries include direct material damage, financial losses resulting from direct material damage, costs related to property decontamination, excluding decontamination and debris containment, business interruption covered by the policy, as a result of material damage.

Reinsurance

The September 11, 2001 terrorist attacks led a majority of reinsurers to exclude the largest risks from Terrorism cover, provided for in Non-Life treaties. This decision had a particularly serious impact on French insurers, who are legally bound to cover all losses caused by acts of terrorism. This led to the opening of negotiations between insurers and reinsurers, under the auspices of the public authorities, with a view to implementing a scheme designed to avoid any cover gaps.

For Large Risks, these negotiations led to the creation, in 2002, of an Economic Interest Grouping (G.I.E.), GAREAT, the purpose of which is to set up a mutual co-reinsurance scheme between its members, providing them with unlimited State-guaranteed cover through CCR.
For small or medium risks, no market agreement has been entered into, but CCR has been authorized by law, since 2006, to offer insurance companies, upon request, unlimited State-guaranteed cover.

Renewal

This framework was negotiated with French State (DGT), representative of French insurance companies (FFA), GAREAT and CCR, for a multiyear period (4 years) in order to insure strong stability of:

- Scheme of reinsurance: Public-Private Partnership between CCR and French Market,
- Attachment points and cost of reinsurance covers provided by CCR and by the

Open Market for the French Market,

- Scope of cover.

These CCR covers, with French State-guarantee, only concerns risks in the scope of the compulsory cover (Article L 126-2 of the French Insurance Code).

However, Insurance companies can provide a largest cover than the compulsory scope but without the French State cover. For example, the Market can provide Contingency Business Interruption and financial losses resulting from indirect material damage, business interruption due to denial of access or geographical scope (French Polynesia, New Caledonia).

Laurent Montador, Executive Vice President.
CCR Group - Caisse Centrale de Réassurance

HACKERS IN THE SKIES: HOW DRONES ARE THE NEW WEAPON FOR ESPIONAGE AND DATA HACKING

(4 minute read)

Unmanned Aerial Vehicles, commonly referred to as drones, have been a source of entertainment for millions of enthusiasts, and a technical resource for many industries to advance their aerial surveillance, mapping, and protection programs. They're bringing new views to light through film and photography, inspecting infrastructure to find vulnerabilities, and even flying in fleets to survey natural disasters, deliver medicine and food, and locate missing persons. For as many positive case uses for drones, there are even more possibilities for the negative, including espionage, spying, warfare, and most recently unfolding, data center hacking.

Significant resources are spent to protect corporations, from ground fences, armed doors and windows, and emergency shutdown systems. Aerial threats are emerging, and without the ability to create an airspace barrier, security officers need to create a drone defence program to prevent attacks on critical infrastructure.

The interruption of a corporation or data centre's operation can cause system malfunctions and server failures, financial damages, including losses by customers, and can diminish brand image and prompt a loss of client confidence. Drones are enabling new avenues for hackers and terrorists, who can use them to carry payloads of any kind. The U.S. Federal Aviation Administration (FAA) and other global regulatory bodies are significantly behind in developing and enforcing regulations to protect vulnerable buildings, and drone operators can easily evade and ignore existing regulations. Organizations with critical infrastructure must be proactive to protect their airspace and vulnerable buildings from unauthorized drone activity.

Drones are becoming a critical part of a hacker's equation introducing a sophisticated level of espionage

Drones are becoming a critical part of a hacker's equation introducing a sophisticated level of espionage

In February 2017, researchers with Ben Gurion University's Cyber Security Research Center demonstrated an alarming hacking technique by using drones to detect vulnerabilities in air-gapped computers installed with malware. Air-gapped computers are developed as a network security measure to ensure that a secured computer network is physically isolated from an unsecured network. However, these researchers demonstrated how air gaps can be breached and data can easily be intercepted by a drone. Once a computer is infected, a drone with a camera can be deployed to hover outside a window, near the hardware. Detected through electromagnetic signals, the transmitting computer can be located by the drone, and capture data through LED signals emitted by the hard drive.

A blinking light on a computer may seem innocuous, and these researchers show that infected computers can be easy to overlook, but programmed to help a drone find its location and prompt a swift and easy transfer of information. If When the drone's camera has line of sight to the target, it will identify the correct computer. It takes only moments for a drone to locate the computer, complete an upload of information, and fly away and out of sight. See the process in action, here. New use cases for drones are being tested every day, and hackers are quick to note how drone technology can support illegal activity. Corporations are on the lookout for new hacking techniques. Those with aerial defense systems in place are best prepared to protect their operations.

Not only are drones laptops in the sky, but they are also a physical risk and can carry hazardous payloads

Security officers are acutely aware that it only takes a few grams of a mysterious powder to be dropped into a cooling unit to prompt a catastrophe. In combat zones, drones have been designed to steadily carry sensitive payloads, anywhere from cameras, medical supplies, and pesticides. Terrorist groups have taken advantage of this, transporting bombs, guns, grenades and deadly chemicals to drop off quickly and without any physical harm to their soldiers. The same risks apply for data centres and corporations, particularly when their rooftops hold cooling units. Drones can be custom built by hackers, designed specifically for spying and infiltrating a network. There's no such thing as an airspace fence, and a $500 drone crashing into a cooling unit could cause millions in damages to climate-controlled hardware.

Drones on the market today can carry upwards of 200 pounds, and can stay in the air for over an hour – enough to fly many miles. A crash could be catastrophic. Without knowing the drone's payload, whether it be a camera or other device, data centre operators need to be aware that any drone in their area is a risk to their operation and employees' safety.

Drone technology and use cases are outpacing federal regulators and law-makers, leaving data centres and other critical infrastructure security officers to decide how to address aerial threats

The FAA estimates small, hobbyist unmanned aerial systems (UAS) purchases may grow from 1.9 million units in 2016 to as many as 4.3 million by 2020. Sales of UAS for commercial purposes are expected to grow from 600,000 in 2016 to 2.7 million by 2020. Combined total hobbyist and commercial UAS sales are expected to rise from 2.5 million in 2016 to 7 million in 2020. This market is growing rapidly, and there are few and inconsistently enforced requirements to register a drone with the FAA.

Federal laws have been written to guard aircraft, including drones, treating them with the same protections as a commercial airliner. It is illegal in most countries to interfere with the operation of or cause physical damage to a drone. This only leaves room to create a defence program. Data centres and organizations with critical infrastructure must not wait for regulators to provide guidance on drone espionage and physical attacks, and regardless of the existence of laws, hackers and terrorists will evade and ignore such regulations.

Data centres must take proactive measures to detect drones and deploy a defence to protect high-risk and high-value infrastructure

Drone protection is no longer theory – it's a practice in place today, since any drone user is capable to cause millions in damages. Drones threaten the physical security of corporations, and consequently, their cybersecurity. They are discreet and capable of carrying payloads of several pounds over fences and right next to structures, including devices to intercept or disrupt data communications or hack into servers.

Unique aerial security risks exist for corporations, as demonstrated through new drone research and hacking programs, and a lack of regulatory protections. With an understanding of the threat that drones pose, as well as a proactive plan in place to protect critical infrastructure, security officers will be a significant step ahead from hackers, spies, and terrorists.

Amit Samani,
Regional Sales Manager
Dedrone

ADDRESSING CYBER CATS THROUGH A PARAMETRIC TRIGGER STRUCTURE

(4 minute read)

The implications data breach can have for a public company are significant and may at first seem too overwhelming to address all at once. However, there are viable solutions for immediate remediation that can benefit the company and its shareholders as well as help to manage public perception of the breach.

Protection Gap Issue

For the last five years we have all heard about high-profile cyber breaches, including at Home Depot, Target, Anthem, and Equifax. Clearly the threat is real and increasingly worrisome. Truth is, these are only the breaches that have been widely publicized; we can't even count the number that have occurred in the last five years.

With this growing threat, companies must consider what they can do to shelter their interests as much as possible from exposure in the event of a breach. The answer? Insurance. Yet for cyber insurance, a new market with evolving risk, it's hard to keep up with the threat—hence the protection gap between exposure and coverage.

Remote Risks—the CATs of the Cyber Industry

While most breaches tend to be small, with minimal consequences for the company, there are outlier cases that keep the C-Suite up at night. Target, for example, reported $310 million in losses related to its data breach in the two years following the event. The company's protection was not even close to ideal, covering less than a third of the loss. A similar situation happened with Home Depot. According to an Advisen article, the breach at the Office of Personnel Management is expected to cost over $1 billion for the three years following the breach.

Equifax's is the latest in a series of breaches that Verisk's Property Claim Services® (PCS®) has analysed, and it's one that had shocking consequences. Erik Gordon, a University of Michigan business professor, says the amount of damages the company will pay just to settle lawsuits related to the breach "will have a "b" in it." It appears that the company has about 12.5 per cent insurance coverage to offset the economic loss, but even this seems insufficient. Plus, there will be immediate remediation costs and additional expenses.

The Pain Point for C-Suites

When a breach happens, corporate executives sound the alarm and the resulting unbudgeted expenses can be considerable, not to mention the impact on share price. The latter is of particular concern to the C-Suite executives because it represents the company's perceived value in the eyes of both the consumer and the long-term investor. A mechanism should be in place to remediate the changes in share price should a breach occur. For example, an insurance play related to share price fluctuations following a breach would provide protection and some peace of mind after an event.

Parametric Share Price solution

The PCS team studied 15 major breach events dating back to 2009. Analysis showed that the longer an event was monitored, the more factors could influence fluctuations in share price. The study also revealed two key points where share price fluctuations and trading volume are correlated:
Share prices drop significantly during the first five days after a breach disclosure—with declines of five percent or more; and then there's

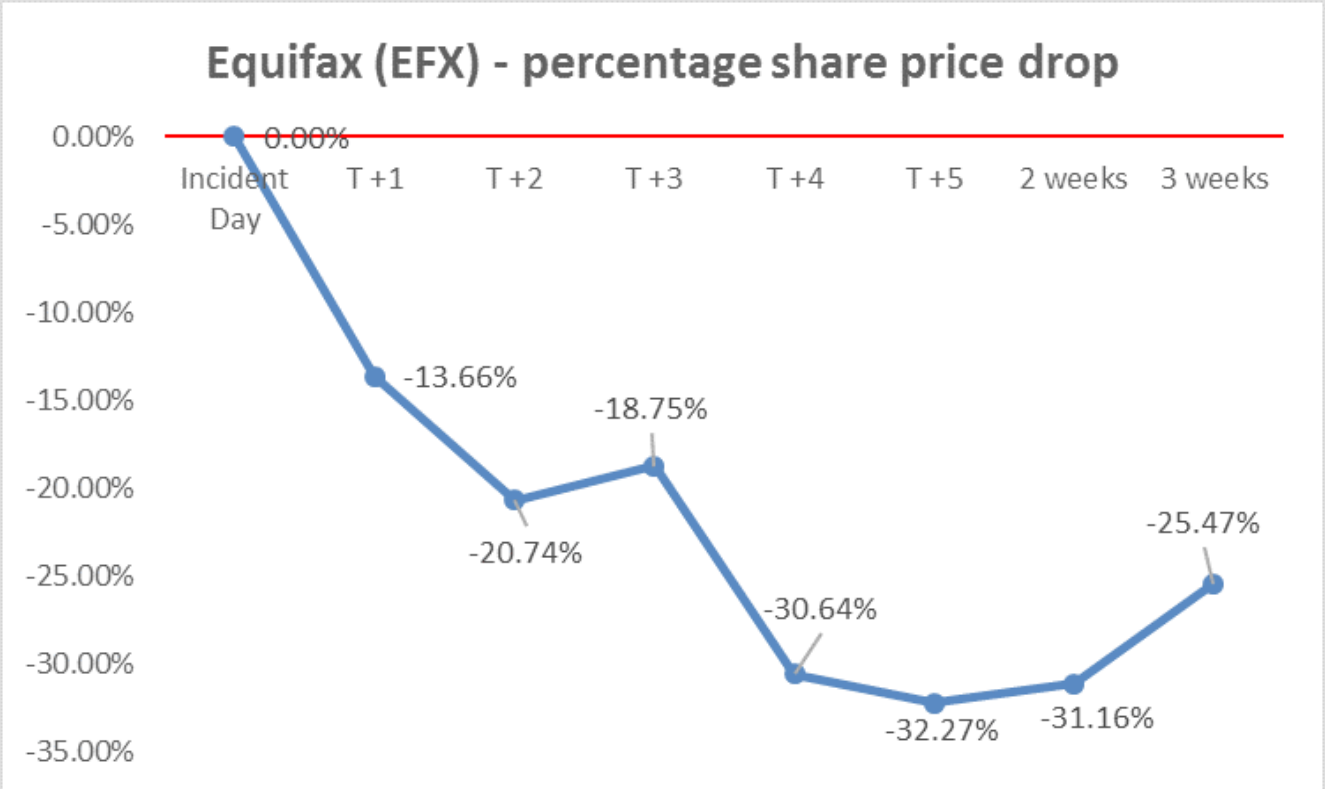
a particular moment later in which similar share price fluctuations occur. These findings led the PCS team to define key points for a parametric trigger trading structure.

Benefits for the Company

As with remote risks that have significant exposure, the parametric trigger trading structure addresses key issues for executives: covering the most extreme breaches, providing protection, and facilitating easy disbursement of capital in a relatively short timeframe. The structure would be easy to understand, considering that it plays on share price and trading volume and provides fast execution at the key timeframe moments, making it easy to define and collect capital at specific points highlighted by the structure.

The Equifax Breach

Taking Equifax as an example, we know that the company's exposure for the breach will probably be north of US $1 billion, while the insurance coverage currently in place is about a tenth of that amount. In such instances, a parametric trigger trading structure would monitor fluctuations of the share price and trading volume and provide disbursement of capital at the triggering points. As we can see in the chart below, Equifax lost about 30 percent of its share price value within the first two weeks after the breach was disclosed. Share price fluctuations indicate a slight recovery, but it remains to be seen what will happen. The final impact will be affected by the responsiveness and perception of the consumer and the market. Until then, the impact on company resources and public image could prove devastating.



Concluding Remarks

In situations of remote risks such as the Equifax event, a parametric trigger would put the company and shareholders at ease and provide capital to address public concerns and implement measures to restore faith in the company among both shareholders and the public. Share price will take a while to recover to pre-breach levels, if it ever does, but the immediate response and the expenses related to the breach could be crucial. With better planning and the use of a parametric trigger structure, the impact could be contained, providing the necessary mechanism to keep the company alive and functioning.

Alex Mican, MBA, ARe, AINS,
Product Development Manager
PCS | ISO Claims Analytics

WITHOUT TERRITORY WHAT WILL THE SO-CALLED ISLAMIC STATE BECOME?

(3 minute read)

Abstract

As success on the ground in Iraq and Syria grows should we be applauding the defeat of the so called Islamic State? Why did Andrew Parker the Director General of MI5 in a recent speech say, "the challenge that we face is undoubtedly a stark one. More threat, coming at us more quickly, and sometimes harder to detect?"
Ed Butler in a recent Pool Re report said, "the expulsion of thousands of foreign fighters along the Euphrates could provide the capability to attack European targets at a higher tempo than before. Domestic and international threats will become increasingly interrelated. These will be further enabled by the exploitation of the internet, social media and end-to-end encryption."
Philip Ingram MBE, a former senior intelligence officer and now freelance journalist, looks at what is happening with so called Islamic State as their physical caliphate gets defeated and he introduces the United Cyber Caliphate.

Article

There has been so much debate over the years as to what to call the so called Islamic State, or ISIS, or ISIL or DAESH as no one wants to give them the state like credence they aspire to, in a name that will stick.

The current ground campaign in Iraq and Syria is certainly squeezing the territory that the so-called Islamic State had trumpeted as the foundations of its state. Certainly 3 years ago it has the trappings of statehood with a taxation system, courts, police, its own welfare, education and health systems and a business plan to grow state like wealth. That has all but gone and stories are emerging of disillusion amongst the fighters facing certain death, but what of the future?

The recruiting arm of the so called Islamic State that has been so successful in encouraging foreign fighters and in some cases their families, to give up everything and go to Syria for "the cause" has been quietly preparing for the current loss of territory.

About 2 years ago, messages started to go out via their recruiting networks telling those who wanted to travel to Syria for the cause, to remain at home and prepare for jihad in their home countries. Of note the initial call went out only to Western based recruits but actively encouraged those from SE Asia still to travel. They were trying to expand their influence deeper into that region.

The so-called Islamic State expansion outside Syria and Iraq has been developing for quite some time. A US National Counter Terrorism Centre map from 2016 shows 18 countries with official branches of ISIS and an additional six countries where there are "aspiring branches" of the terror group.

If that were not enough, there is a war of words going on in some closed discussion groups between Al Qaeda, (no they haven't gone away) and so called Islamic State groups vying for who can do the worst. There are clear indications that Al Qaeda are in the ascendancy again, albeit slowly, and want to commit another 9/11 type atrocity.

Putting Al Qaeda to one side, as the physical so-called caliphate in Iraq and Syria gets squeezed and eventually dies, which it will, where will the direction, training, command and control for their frightening brand of extremism come from? Well that mechanism already exists. It is called the United Cyber Caliphate. What we are seeing is a transition from a so-called "physical caliphate" to one in cyberspace, the "virtual caliphate."

This transition, for western countries in particular, is of great concern. Their grooming networks, on line training facilities, propaganda and reach is frightening, in both its scale and quality. Their online courses include not just how to make bombs but how to evade surveillance, how to create anonymous encrypted communication networks and more.

These networks are huge, the cyber intelligence company, Global Intelligence Insight is monitoring over 120 of them with thousands of users in total communicating through them. Vasco Da Cruz Amador, its CEO says, "we are only scratching the surface of the online issue and the amount of activity is frightening."

According to the October 17 report "BEYOND THE CALIPHATE: Foreign Fighters and the Threat of Returnees" by The Soufan Centre think tank, there are now at least 5,600 citizens or residents from 33 countries who have returned home from fighting in Iraq and Syria. Added to the unknown numbers from other countries, this represents a huge challenge for security and law enforcement entities. Ed Butler in a recent Pool Re report said, "the expulsion of thousands of foreign fighters along the Euphrates could provide the capability to attack European targets at a higher tempo than before. Domestic and international threats will become increasingly interrelated, and these will be further enabled by the exploitation of the Internet, social media and end-to-end encryption."
The rise of a command capability in the United Cyber Caliphate (UCC) can only be worrying as is the possibility of less scrupulous states assisting the UCC in its actions to encourage and enable further terror attacks in Western countries, but that theme is a whole new article.

Philip Ingram MBE is a former senior intelligence officer but now journalist who has been writing on intelligence, security and geopolitical issues for some years. He maintains access to organisations who monitor global and terrorist threats. He is a sometime commentator for the BBC on both television and radio and is used by other international channels for professional comment. He runs his own content providing company Grey Hare Media

COUNTERFACTUAL ANALYSIS OF THE 2017 BARCELONA TERRORIST ATTACK

(16 minute read)

Abstract

On Thursday afternoon, 17 August 2017, a white Fiat Talento van rammed into pedestrians on Las Ramblas, the world-renowned boulevard in central Barcelona. The young Moroccan van driver, Younis Abouyaacoub, zigzagged to strike as many people as possible, knocking many to the ground and sending others fleeing for shelter. The death toll was fourteen and another hundred were injured. About eight hours later, a blue Audi A3 car ploughed into pedestrians in the popular seaside resort town of Cambrils, 110km south-west of Barcelona. The ramming vehicle overturned and five people got out, wearing fake suicide vests. The terrorists started stabbing passers-by. A woman was critically injured and later died in hospital. Five other civilians and a police officer were hurt. The terrorists were shot by police; four died at the scene and one later died of his injuries.

This might be classified as a successful terrorist attack, since the plot was not interdicted by the police or security services. However, the attack actually improvised terrorist Plan B. Counterfactually, the more ambitious and technically demanding Plan A might have resulted in the worst terrorist atrocity against the western alliance since 9/11. This original plan involved weaponizing three vans each fully loaded with forty 32 kg butane gas cylinders, which would have been driven into the cathedral, the port and Las Ramblas. Fortuitously, an explosive accident in the terrorist bomb factory wrecked this original plan, and the terrorists resorted to the simpler more reliable alternative tactic of switching from chemical energy to the kinetic energy of vehicles to ram pedestrians.

The Attack

At 4.56pm on Thursday afternoon, 17 August 2017, a white Fiat Talento van rammed into pedestrians on Las Ramblas, the world renowned boulevard in central Barcelona that extends for over a kilometre and draws crowds of tourists. The young Moroccan van driver, Younis Abouyaacoub, zigzagged to strike as many people as possible, knocking many to the ground and sending others fleeing for shelter in local shops and cafés. The death toll was fourteen, one as young as seven, and another hundred were injured.

About eight hours later, a blue Audi A3 car ploughed into pedestrians in the popular seaside resort town of Cambrils, 110km south-west of Barcelona. The ramming vehicle overturned and five people got out, wearing fake suicide vests. The terrorists, who had bought knives and an axe a few hours beforehand, started stabbing passers-by. A woman was critically injured and later died in hospital. Five other civilians and a police officer were hurt. The terrorists were shot by police; four died at the scene and one later died of his injuries.

Counterfactually, the terrorist plot might well have been interdicted by Los Mossos, the Catalonian regional police force. As recently as June 2017, the CIA had warned that Barcelona was a top target for Islamist militants, and even specified the heightened risk to Las Ramblas. Most terrorist attacks against the western alliance, including Spain, are stopped by the security services, especially the larger ambitious plots: too many terrorists spoil the plot. What made this particular plot more difficult to interdict was its compact network profile: all the conspirators lived in or around the same small town in Catalonia close to the French border, and shared not only the same Moroccan background and heritage, but most of the cell members played in the same soccer team, and came from just three extended families. As shown by other terrorist plots against the

western alliance, the more extensive the kinship, and the more close-knit the cell, the fewer communications that can be intercepted by electronic surveillance, and the harder it is for a mole to uncover the plot. The terrorists would have been confident that their major plot, ambitious as it was, had a reasonable chance of eluding Los Mossos.

The interdiction of the attack is an upward counterfactual; an alternative realization of the past where things were better than they actually were. A downward counterfactual (i.e. an alternative realization where things were worse), would be where the terrorists implemented their original plan of weaponizing three vans each fully loaded with forty 32 kg butane gas cylinders. An explosive accident in the terrorist bomb factory wrecked this original plan, and the terrorists resorted to the simpler more reliable alternative tactic of switching from chemical energy to the kinetic energy of vehicles to ram pedestrians.

The Return of Al Andalus

Spain has a special allure for Islamists that is engrained deeply in its mediaeval history. Starting with the invasion of Gibraltar in 711, less than 80 years after the death of the Prophet, between the 8th and 15th centuries, a large part of the Iberian Peninsula was ruled by Muslim caliphs. Extremist websites call for a return to the golden era of Al Andalus, as mediaeval Spain was known, when Islamic culture flourished and Islamic civilization reached its zenith.

Throughout modern history, there has always been a Muslim community in Spain. This has expanded with growing economic development in Spain. A small number of Muslims migrated to Spain from Syria in the early 1980s. One who fled the assault by Syrian president Hafez Al Assad against the Muslim Brotherhood was Abu Dahdah. He made contact with Al Qaeda affiliates elsewhere in Europe, and welcomed Jihadis from Bosnia, Chechnya and Afghanistan. Abu Dahdah hosted an Al Qaeda meeting in Spain a couple months before 9/11. For this meeting, one of the World Trade Center attack pilots, Mohammed Atta, stayed in a hotel in Salou, which happens to be close to Cambrils, the scene of the second van ramming attack on 18 August 2017. This was home territory for Islamist militants.

Despite its efforts at integration, not least in Catalonia, Spain has struggled with extremism inside its Moroccan community, in much the same way as Britain has struggled with its Pakistani community and France with residents of Tunisian or Algerian descent. That problem is linked to Spain's close ties with Morocco, which accounts for much of the country's Muslim migration, especially during the 1990s. Moroccans had key roles in the 11 March 2004 Madrid bombings, which killed 192 people and wounded several thousand. One of the organizers and masterminds was Jamal Ahmidan, nicknamed 'el chino' because of his oriental almond eyes. His Moroccan friend and fellow drug peddler and conspirator was Rachid Aglif, nicknamed 'el conejo' because of his rabbit-like facial features. The casual familiarity of these nicknames reflects the deep bonds of trust and camaraderie that characterize the resiliency of dual drug and terrorist networks.

Catalonia has become increasingly known as a centre of extremism, with almost one third of ISIS-linked arrests in Spain made there. A 2007 cable from the US State Department warned of the risk of radicalization in Catalonia and called for a regional counter-terrorism hub to be set up in Barcelona. Published openly by Wikileaks, this cable stated that Spanish and American authorities had identified the region as a major Mediterranean centre of radical Islamist activity that had attracted terrorist recruiters. The US State Department suggested that men with a North African background, at heightened risk of radicalization, would provide fertile ground for terrorist recruitment. The economic boom in Catalonia, home to just over a quarter of Spain's almost two million Muslim residents, has attracted large numbers of Muslim migrants from Morocco, Algeria and South Asia.

But many have struggled to integrate and have been drawn to clusters of radical Salafi mosques.

For more than a decade since 2004, Spain has been successful in preventing the kind of Islamist violence that has afflicted its western European allies. However, in 2016, a Spanish Interior Ministry report noted that the numbers of messages on Jihadi propaganda networks calling on volunteers to launch attacks on Spain and to liberate cities such as Toledo, Córdoba, and Seville had doubled compared with previous years. It also noted that ISIS had begun to translate its media material into Spanish. It has recruited in Spain, aided by the strong links with Morocco. From that North African territory, more than a thousand volunteers are estimated to have travelled to the ISIS conflict zones in Iraq and Syria.

By contrast, a modest number of around 170 Spanish Muslims have gone to fight in Syria. This is a lower number than some other European states, but the whereabouts of most of them are unknown. In addition the Spanish security agencies are monitoring 1,100 people with extremist views. The country is also currently receiving large numbers of refugees from North Africa. Although the vast majority are genuinely seeking refugee status, as it loses its bases in Libya, ISIS is trying to infiltrate fighters into Europe within the refugee exodus.

The Ringleader: Imam Abdelbaki Es Satty

Europol figures show that, in 2015, Spain had the second highest number of Islamist terrorist arrests, with 187. France was top with 424. However, the Muslim community makes up only 2.1% of the population in Spain compared to 7.5% in France. So in the year which is remembered for the Charlie Hebdo committee assassination on 7 January and the Paris stadium, theatre, and café attacks on 15 November, as a percentage of its Muslim population, Spain actually faced a more sizeable potential terrorist threat than France.

An increasing prison population of Jihadis spreads more rapidly and persistently the contagion of radicalization to other inmates. As in other countries, Spanish prisons have become a fertile recruiting ground for Islamist extremism. Jailed Jihadis are able to indoctrinate, and radicalize other prisoners, who may have been convicted of offences unrelated to terrorism. This applies to all penal systems. Khalid Masood, the Westminster lone-wolf terrorist of 22 March 2017, converted to Islam in an English prison, where he was serving time for stabbing offences.

Acquaintances of the 42 year-old imam Abdelbaki Es Satty said he was not religious until he was jailed for smuggling hashish between Morocco and Spain, and breaking Spanish immigration laws. Es Satty spent several years in prison, during which time he befriended Rachid Aglif. Easily recognized as 'el conejo', Aglif was serving 18 years for his part in the 11 March 2004 Madrid bombings. He had helped procure explosives stolen from mines in Asturias. As a fellow Moroccan drugs peddler, Abdelbaki Es Satty had much in common with Rachid Aglif.

After release from jail in April 2014, the Islamic preacher should have been expelled in accordance with Spanish immigration laws. However, he won an appeal against deportation by convincing a judge that this was against international law. He followed up his court win by seeking asylum through lawyers in an application filed on 29 November 2014. This allowed him the freedom to travel around Europe. As has happened elsewhere in Europe, in deportation cases involving foreign criminals, there has been a public outcry in Spain over criminal exploitation of human rights law.

Es Satty spent several months trying to find employment at mosques in Brussels' Vilvoorde district in the north of the city. He lived there for several months from January 2016, and would have been there at the time of the Brussels airport bombing of 22 March 2016. Vilvoorde is notorious for Islamist

activity, and sending residents to fight for ISIS in Syria and Iraq. When Belgian police were informed by locals of Es Satty's attempts to get work, and contacted the Catalan department of justice, they were mistakenly told he had no links to extremist violence. Unfortunately, the Catalan police officer who answered the informal request for information from Belgium did not have the complete records on Es Satty. The fact that the Catalan interior ministry was warned by Belgian authorities in March 2016 about Abdelbaki Es Satty shows that he was on their security radar screen to some extent.

In 2015, Es Satty started teaching at one of the two mosques in Ripoll, a quiet Spanish town in the north-east of the country at the foothills of the Pyrenees near to the French border, and around 62 miles from Barcelona. The small Muslim community of a town, proud of its Catalan identity, consists of about 500 people out of a population of 10,000. The imam repeatedly preached about Jihad and killing infidels, and exerted a strong addictive hold on a number of impressionable local young Muslims, especially during Ramadan. They succumbed to his gift of eloquent persuasion and eventually became members of his Ripoll terrorist cell. Before he quit in June 2017, Es Satty had succeeded in radicalizing a close-knit group of around eight men and boys, several of whose families hailed from the same small town of M'rirt in central Morocco. The common ethnic, language, family and geographical bonds made this cell highly compact and resilient against counter-terrorism penetration. Accordingly, Spanish police did not have the imam nor other members of the Ripoll terror cell under surveillance, despite Es Satty's extremist connections and their prior knowledge of his criminal background.
In Ripoll, Es Satty's spartan accommodation was hardly more comfortable than a prison cell. He left it on Tuesday, 15 August, expecting never to return. But instead of the theatrical public martyr's death he sought by immolation in a fireball explosion at an iconic location in Barcelona, he died the next day anonymously in an accidental explosion, whilst preparing explosives in a safe house in Alcanar, a quiet beach town 200km south of Barcelona. Traces of the high explosive, triacetone triperoxide (TATP), were found in the house, which was owned by a bank and was being occupied illegally. The remains of Es Satty and another bomb-maker were found in the house, along with some ISIS documents.

Other Cell Members

In July 2017, some sixty imams from various European countries embarked on a tour of terrorized cities, including Berlin, Brussels, Toulouse and Nice, in order to promote Islam as a religion of peace. Whilst the great majority of imams endorse this peaceful initiative, there are also some radical imams who espouse extremist violent views. They have been central to the international spread of Islamist doctrine, although few have been directly involved themselves as operatives in terrorist attacks. An exception has been Abdelbaki Es Satty.

Abdelbaki Es Satty appreciated the security value of keeping his terrorist plot a well-guarded secret known only to a small close-knit group of those who could be entrusted with a martyrdom mission. Nine of the ten individuals named below come from just three families. Two of those listed, Driss Oukabir and Mohammed Aalla, were brothers of active operatives who were killed by the police. They both had an important auxiliary role in vehicle procurement, although their knowledge of the plot may have been quite limited. The brothers Driss and Moussa Oukabir. Driss rented three vehicles in a town about 25km from the centre of Barcelona. Following the attack, he was arrested in Ripoll, where he lived. He had previously spent prison time in Figueres, Catalonia, and had been released in 2012. His teenage brother, Moussa Oukabir, was among the five killed by police in the coastal town of Cambrils. He outed himself as a Jihadi on social media, where he posted extremist views such as wanting to kill unbelievers and leave only Muslims who follow their religion.

The brothers Omar and Mohamed Hychami were both in the second vehicle in Cambrils. Their father blamed imam Abdelbaki Es Satty for brainwashing his sons, who both lived in Ripoll. This is literally true. According to the Cambridge English dictionary, brainwashing is the act of making someone believe something by repeatedly telling them that it is true, and preventing any other information from reaching them. Es Satty taught Arabic to children in Ripoll. A former classmate recalls the Hychami brothers speaking together in Arabic rather than Catalan. It is quite credible that what they learned in Arabic came mostly from the imam.

The brothers Houssaine and Younes Abouyaaqoub were first cousins of the Hychami brothers. They had last visited their ancestral home in Morocco in March 2017. Houssaine died in the second vehicle in Cambrils. Younes had the privilege and responsibility of the primary strike role of driving the van that rammed pedestrians on Las Ramblas on Thursday afternoon, 17 August, and was later killed in police action after his getaway from Barcelona, and escape on the run.

The brothers Said, Mohammed and Youssef Aalla. Said Aalla was made class delegate at his school because of the trust and confidence he inspired. He died in the second ramming vehicle in Cambrils. This car happened to be owned by his brother Mohammed, who had no martyrdom role, and may have had scant knowledge of the plot. By contrast, the third brother, Youssef, was a bombmaker and died in the accidental blast in Alcanar on 16 August.
Mohamed Houli Chemlal was originally from Melilla, a Spanish autonomous territory on the Moroccan coast, and also lived in Ripoll. A bomb-maker, he was injured in the explosion in the house in Alcanar, from which he was extricated and then arrested. He admitted that a larger attack was planned before the militants' plot went wrong.

Terrorist Attack Interdiction

Almost all of the prime suspects in the Barcelona and Cambrils attacks have been identified as Moroccans or of Moroccan origin. That is the same background as the ringleader of the Paris attack on 13 November 2015, as well as of the men who brought suitcase bombs into Brussels airport on 22 March 2016. It was also the nationality of Ayoub El-Khazzani, who would have shot many passengers on a Thalys inter-city train between Amsterdam and Paris on 21 August 2015, had his AK47 not jammed.

Over 1,600 Moroccans have joined ISIS in Syria and Libya, and security experts believe there are hundreds of sympathizers inside the country. Spanish counter-terrorism relies heavily on cooperation with the Moroccan security forces, who have successfully penetrated migrant communities across Europe through a strong network of informants, despite concerns from human rights groups about their methods. But that assistance also depends on good diplomatic relationship between the neighbouring countries, which has been frayed over Ceuta and Melilla, Spain's outposts in North Africa, and the dispute over the Western Sahara region.

Despite the costs in times of austerity, the Spanish government has raised both the staff numbers and the budget for its intelligence services. Before 11 March 2004, the number of security agents assigned to investigate Islamist extremism was just a few hundred. Now it stands at 3,000. Aggressive counter-terrorism legislation has allowed the authorities to arrest suspects at an early stage of attack planning. More than 700 jihadi suspects have been arrested since 2004. Of those, some 200 have been detained since Spain last raised its terrorism threat level in June 2015. Sometimes dismantling cells quickly produces inconclusive judicial results because of scant courtroom evidence. In 2008, French authorities were dismayed when Spanish police used testimony from one of their agents to break up a cell mainly comprising Pakistanis in Barcelona, although no explosives were ever found. However, eleven men were convicted of plotting to bomb the city's metro, but at the

loss of the French mole's cover. Prepared to take such sensitive and forthright counter-terrorism decisions, Spain successfully managed for 13 years to avoid any loss of life from jihadi terrorist attacks.

Counter-terrorism collaboration between the French and Spanish authorities needs to be at its closest in the border region between France and Spain. In the small Catalonian town of Ripoll, not far from the French border, Abdelbaki Es Satty diligently evolved his ambitious Barcelona plot over a period of about a year, without detection by the French or Spanish authorities. Police authority in dealing with this plot lay with the regional Catalan police force, Los Mossos d'Esquadra. They have replaced Spain's Policia Nacional and Guardia Civil within the territory of Catalonia. In particular, Los Mossos are responsible for policing in the city of Barcelona. In the past, Catalonia's government and police have complained about the exclusion of Los Mossos from international meetings on terrorism because they are not a national force. The day after the attack, national and Catalan authorities held separate crisis meetings. This situation would be akin to that in UK if Scotland were to become independent - there is ambivalence over the sharing of MI5 intelligence with an independent Scottish government. Inevitably, Catalonian secessionism has surfaced as a factor in post-attack analysis. The Catalan president accused the Spanish government of playing politics with security by restricting funding for extra Catalan police, and denying access to Europol.
Los Mossos have come under scrutiny for taking ten hours to send bomb experts to the scene of the explosion in Alcanar, so delaying the discovery of the militant cell. Los Mossos suspected that a gas leak or narcotics laboratory was the cause of the blast, which tore through the house near midnight on Wednesday, 16 August. Police had noticed not just butane gas cylinders, but also acetone - a compound used in laboratories to produce drugs. However, the full evidence did not support this hypothesis. Explosives experts from the Spanish Guardia Civil would have been of assistance in discovering earlier what was really going on in the destroyed house in Alcanar. Terrorism experts have offered the counterfactual speculation that if Los Mossos had discovered the presence of militants at the house in Alcanar more quickly, they might have had time to raise the alarm, alert the regional law enforcement services, and perhaps even foil the lethal van attack in Barcelona.
Vehicle-borne Gas versus Fertilizer Bombs

Vehicle-borne Improvised Explosive Devices (VBIED) have been called the terrorists' air force because of their strategic importance. For imam Abdelbaki Es Satty and his compact Ripoll terrorist cell, plan A was the preparation of three VBIEDs, vans packed with butane gas canisters, which could be driven at speed against the Sagrada Familia cathedral, Las Ramblas, and an iconic target in the port of Barcelona. The cell initially attempted to hire a much bigger vehicle than a van, but did not possess the correct HGV permit.

The cell purchased about 500 litres of acetone to manufacture the explosive Triacetone Triperoxide (TATP), called the Mother-of-Satan because of its dangerous and temperamental volatility. The other ingredients are hydrogen peroxide and sulphuric acid. TATP is favoured by terrorists for its ability to evade detection aimed at nitrogenous explosives, and due to its low cost and the comparative ease with which its ingredients can be procured. Traces of TATP were found alongside around 120 large 32kg butane gas canisters in the ruins in Alcanar. TATP has been widely used before in terrorist bombings, most recently in the rucksack bomb of Salman Abedi in his suicide attack on the Manchester Arena of 22 May 2017. Gas canisters themselves are stable by design, but can explode if detonated using TATP explosives.

Counterfactually, if the terrorists' original plan had succeeded, the death toll might have been more than an order of magnitude higher than it was. Each of the three vans

would have been packed with forty 32 kg gas canisters – more than a ton of butane gas. Upon successful detonation, a powerful vapour cloud explosion and massive fireball could have been generated. Driven at speed into a densely crowded public place, each van might have killed about fifty people, as well as badly injured and burned many more.

It only requires one operative to drive each of the three propane gas vans. Others in the cell could have achieved the martyrdom they sought, and secured their place in Paradise, by riding as passengers in these vans. But they could have pro-actively amplified the attack and compounded the mayhem by donning suicide vests, and exploding these amongst the crowds in Barcelona. It is known that the cell procured detonators and shrapnel to make suicide vests. One suicide vest packed with explosives was actually found in the rubble of the bomb factory in Alcanar. Accordingly, the overall impact of multiple bombs being exploded in Barcelona might have been a death toll well exceeding that of the 2004 Madrid bombings, and would have been as politically and economically devastating.

Part of the value of counterfactual terrorism risk analysis is the insight it affords into targeting and weapon selection. International name recognition has long been recognized as a key criterion for targeting. One of those arrested, bomb-maker Mohamed Houli Chemlal, has affirmed this by stating that the plan was to use explosives against Barcelona monuments, including the Sagrada Familia cathedral, which is the most visited tourist attraction in Barcelona, with 4.5 million visitors in 2016. The annual construction budget of this unfinished structure is approximately €25 million, only part of which is covered by visitor entry fees. Damage would likely have severely impacted the cathedral's finances, the city's tourist economy, as well as Spain's cultural heritage. Ironically, the future prospects for tourism in Morocco, the home country of the terrorists, are quite positive in 2017.

Given knowledge of this explicit terrorist targeting, cathedrals in Germany have since been placed on alert for a potential ISIS attack. Earlier, in September 2016, Notre Dame cathedral in Paris was targeted for a gas cylinder attack; near the cathedral, a car with seven gas cylinders was abandoned. The choice of weaponry is significant. This mode of terrorist attack has been attempted a number of times in countries of the western alliance, notably in Haymarket, London, on 29 June 2007 and Times Square, New York, on 1 May 2010.

The procurement of gas cylinders is far easier than obtaining large quantities of fertilizer for an ammonium nitrate bomb. There are sufficiently many practical uses of gas cylinders for outdoor cooking and barbecue usage that limiting sales would not be practical or effective. However, fertilizer is only used for horticultural or agricultural purposes, and sales of large quantities of ammonium nitrate are tightly restricted. Given these restrictions, the accumulation of enough for even a car bomb would run a high risk of arrest by counter-terrorism forces in the western alliance. One notorious exception has been the Norwegian white supremacist terrorist Anders Breivik, whose lack of basic agricultural knowledge was all too apparent to his farming neighbours. But they were oblivious of the domestic terrorist threat, and failed to alert the Norwegian authorities in time to prevent his vehicle bombing of Oslo government buildings in July 2011.

What is challenging in the deployment of a gas vehicle bomb is mastery of the necessary technique to detonate the gas cylinders using TATP explosive. As shown on Wednesday 16 August 2017 in Alcanar, handling TATP is both technically difficult and dangerous, befitting its name 'The Mother of Satan'. Experience is ideally gained in a terrorist training camp, but there are international travel barriers to obtaining the necessary experience. Terrorists always learn adaptively from the experience of other terrorists. The unsuccessful TATP experience of Abdelbaki Es Satty may discourage other terrorists

from aspiring to use VBIEDs. Vehicle ramming is much more dependable and far less expensive. Furthermore, it requires no training or preparation, apart from route reconnaissance. A clean credit card and a Heavy Goods Vehicle license would be an advantage.

According to an ISIS slogan: half of Jihad is media. The terrorists' alternative Plan B turned out to be sufficiently successful as to achieve the worldwide media publicity they were seeking, even if the ultimate loss outcome was far below the level of their original ambition. Just over a week after they opted for Plan B, on Saturday, 26 August, half a million marched through Barcelona, carrying banners proclaiming in Catalan 'I am not afraid'. King Felipe VI, Prime Minister Mariano Rajoy, and the head of Catalonia's regional government, walked in the crowd led by shopkeepers and residents of Las Ramblas. Such a national response may not have been much less newsworthy than if Plan A had worked out.

Conclusion

A triple vehicle gas cylinder plot, accompanied by a group of suicide bombers, has not been successfully realized as a terrorist attack against the western alliance. Counterfactually, had it not been for an accidental explosion in the house in Alcanar used as a bomb factory, it might have been realized on 17 August 2017. Counterfactual histories are scenarios of the future, The kind of plot conceived to attack Barcelona could be replicated to attack another major city elsewhere in the western alliance.

Vehicle ramming continues to be a reliable and effective lethal terrorist weapon, capable of generating global mass media publicity. The fact that the ramming of pedestrians on Las Ramblas could have been organized at only one day's notice shows how convenient and flexible a weapon it is; one that is hard for security services to stop.

Terrorists follow the path of least resistance in their operations. The logistical difficulty in the terrorist procurement of large quantities of ammonium nitrate fertiliser has encouraged the substitution of gas cylinders for vehicle borne improvised explosive devices. As Salman Abedi demonstrated in Manchester three months earlier, it is possible for a Jihadi to receive training (in Libya in his case), then to make a viable TATP bomb in his home town, and deploy it as planned. So further attempts at weaponizing a propane gas vehicle bomb can be anticipated.

However, the technical failure of the Barcelona vehicle gas cylinder plot should encourage the further substitution of vehicle ramming as an attack weapon. Irrespective of how many protective barriers may be installed to shield crowded places popular with tourists, unprotected crowded places will always remain, and major cities in the western alliance will continue to be vulnerable to sporadic vehicle ramming attacks.

The five operatives in the second ramming vehicle in Cambrils planned to follow the precedent of the three London Bridge Jihadis on 3 June 2017 in using knives in a final act of bloody camera-ready violence to achieve their martyrdom, and win a final accolade from ISIS, who claimed responsibility for the attack. More Jihadi attacks in Spain will be planned. This has already been threatened by ISIS in their long-term objective, publicized by video: 'With God's permission, Al Andalus will once again be the land of the caliphate'.

Dr Gordon Woo Catastrophist, RMS,
Co-Founder & Editor,
Journal of Terrorism and Cyber Insurance.

LEGAL

The Journal, its Management Team, Advisory Board and Sponsors do not purport to provide any advice which is legally binding in the process of producing or disseminating the Journal or any information contained within the Journal and should not be relied upon as a sole basis upon which insurance policies are underwritten. It is the expectation that each (re)insurer will do their own due diligence and use the information merely as an aid to understanding the risks and landscape upon which terrorism and cyber insurance is currently offered. Any information provided by the Journal should be used solely for educational purposes. The Journal cannot guarantee the accuracy of all detail within individual articles, rather the contributors individually guarantee the authenticity and originality of the work contributed. Further any of the contributors in providing an article, warrant that the Journal is their own work and does not breach any laws including copyright and/ or intellectual property laws.

Legally and from an operational perspective, the Journal is a neutral central party used to co-ordinate ideas, research and promote innovation. The Journal retains the legal rights to republish the research, infographics and any images provided to it from contributors, however each contributor may seek the permission of the Journal to subsequently publish their work in other mediums. Similarly, if the article has been published previously in a similar format the author warrants that they have permission to have the article republished in the Journal.