CENTRE FOR SCIENCE
& SECURITY STUDIES

KING'S College LONDON

Radicalisation and Preventative Measures

An Educational Handbook of Insider Threat Case Studies

Geoffrey Chapman, Christopher Hobbs, Zenobia Homan,
Dounia Mahlouly, Daniel Salisbury & Sarah Tzinieris

SEPTEMBER 2018

Introduction

This handbook explores potential routes to malicious insider actions with a focus on radicalisation and violent extremism. It uses a series of real life case studies drawn from different industries to identify the motivations, intentions and capabilities of individuals and groups. It also discusses the different security measures that can be implemented at an organisational level to mitigate the risk posed by staff that may become insiders during the course of their employment, examining their deployment in several sectors. Here the focus is on what the International Atomic Energy Agency (IAEA) term 'preventative measures', or security processes that organisations can put in place to minimise the likelihood of an internal adversary initiating a malicious act. There also exists 'protective measures' that can be put in place to detect, delay and apprehend an adversary once a malicious act has been initiated. A discussion of protective measures and their implementation when faced with both external and internal threats can be found in previous Centre for Science and Security Studies (CSSS) handbooks.[1] Preventative measures, considered in this context, should also not be confused with broader societal level preventative counter-terrorism policies. For example, the 'Prevent' strand of the United Kingdom's Strategy for Countering Terrorism (CONTEST), which aims to combat terrorism by tackling its underlying roots through challenging the narratives associated with violent extremismand supporting vulnerable individuals. While these actions can serve to reduce the risk of radicalisation, they are outside the scope of this handbook.

The case studies in this handbook are intended to serve as a useful resource for nuclear security educators and trainers, and to this end they are presented with accompanying discussion points. This is the third educational case study handbook produced by CSSS in the area of insider threats, security culture and protective and preventative measures.[2] Readers are encouraged to also review these publications for additional cases, discussion regarding the pedagogical benefits of case studies, and guidance on how these can be integrated into nuclear security courses. This handbook starts with a brief summary of the current threat environment, an overview of the phenomenon of radicalisation, and an introduction to preventative measures. These are followed by the specific case studies.

We are grateful to Hannah Kershaw from CSSS for initial proofreading. We hope this will be a useful resource, and educators and trainers interested in developing additional case studies are encouraged to get in touch with the authors.

1 For previous handbooks and other education resources, see King's College London, Centre for Science and Security Studies, 'Teaching and Education – Resources' (2018). Available online at: https://www.kcl.ac.uk/ sspp/departments/warstudies/research/groups/csss/teached/resources.aspx [last accessed 13.09.2018].
2 Ibid.

Glossary

AMWA	American Metropolitian Water Agencies
CIA	U.S. Central Intelligece Agency
CIPAG	U.S. Critical Infrastructure Protection Advisory Group
CONTEST	UK Counter-terrorism Strategy
CVE	Countering Violent Extremism
DHS	U.S. Department for Homeland Security
DUI	Driving Under the Influence
EASA	European Aviation Safety Agency
EU	European Union
FAA	U.S. Federal Aviation Administration
FBI	U.S. Federal Bureau of Investigation
FSB	Federal Security Service of the Russian Federation
FSK	Russian Federal Counter-intelligence Service (formerly the KGB)
GAO	U.S. Government of Accountability Office
GPS	Global Positioning System
IAEA	International Atomoic Energy Agency
ICAO	International Civil Aviation Organisation
ISIS	Islamic State
LBA	Luftfahrt-Bundesamt (German state aviation regulator)
NATO	North Atlantic Treaty Organisation
NEFA	Nine Eleven Finding Answers Foundation
NGO	Non-Governmental Organisation
NIPC	U.S. National Infrastructure Protection Centre
NISA	Somalian National Intelligence and Security Agency
NOI	Nation of Islam
NRD	U.S. Naval Recruiting District
NSA	U.S. National Security Agency
NTSB	U.S. National Transportation Safety Board
OPM	Office of Personal Management
PTSD	Post-Traumatic Stress Disorder
PVE	Preventing Violent Extremism
RapBack	Record of Arrest and Prosecution Background (FBI programme)
ROTC	U.S. Reserve Officers' Training Corp
SAAIA	Somalia's Air Accident Investigation Authority
SCAMA	Somalia Civil Aviation and Meteorological Agency
SIC	Special Regular Medical Examination
SIDA	Security Identification Display Area
SPOT	Screening of Passengers by Observation Techniques
TSA	U.S. Transport Security Administration
UN	United Nations
USEPA	United States Environmental Protection Agency
USIS	United States Investigations Service
9/11	Al-Qaeda terrorist attacks of 11 September 2001

Table of contents

INTRODUCTION.....03

GLOSSARY.....04

Executive Summary.....07

The New Threat Environment 08

Introduction to Radicalisation 10

Overview of Preventative Measures 13

Insider Threats in the U.S. Military

Introduction 15

Case Study 1 16
Attack at United States Military Base, Kuwait

Case Study 2 19
Attack at Military Naval Yard, United States

Case Study 3 23
Theft of Classified Information from United States Military

Insider Incidents in the Russian Northern Fleet

Introduction 29

Case Study 4 30
Theft of Enriched Uranium at Sevmorput Shipyard, Russia

Case Study 5 35
Incident at Gadzhiyevo Naval Base Incident, Russia

Recap and Broader Issues 38

Insider Threats in the Aviation Industry and Other Critical Infrastructure

Introduction 41

Case Study 6 42
Airport Security and Preventative Measures in the United States

Case Study 7 47
German Wings Murder-Suicide Crash

Case Study 8 53
Bombing of Daallo Airlines Flight 159, Somalia

Case Study 9 56
Greenfield Water Reclamation Plant Sabotage, United States

Summary 63

Executive Summary

The New Threat Environment

The tragic and largely unforeseen terrorist attacks of September 11, 2001 had a major impact on strengthening security at critical infrastructure globally. Over the last approximately two decades, national authorities have stepped up counter-terrorism efforts and intelligence sharing, while operators have deployed both new and strengthened security measures. Nevertheless, the terrorism genie is decisively out of the bottle. Jihadist organisations have proliferated through their diffuse international networks, a process that has fatefully coincided with the emergence of digital communications. Terrorist masterminds have successfully employed social media networks to radicalise adherents on a global scale and, unlike the hierarchical and removed al-Qaeda leaders of the past, contemporary manifestations of the same ideology are democratic, decentralised and accessible.

> **"WE HAVE MOVED FROM A WORLD OF TERRORIST-DIRECTED ATTACKS TO A WORLD THAT ALSO INCLUDES THE THREAT OF TERRORIST-INSPIRED ATTACKS"**

The modern devotee is encouraged to engage in small-scale and 'lone wolf' attacks, enabling terrorist groups to reap a propaganda windfall in their effortless 'claim' to such attacks. Gone are the shadowy middlemen who financed and coordinated sophisticated terrorist plots; the new modus operandi is the dissemination of 'inspirational' content through social media, alongside bomb-making instructions that reference everyday household products.

The dismantling of the so-called Islamic State in Iraq and Syria (ISIS) has perversely heightened homegrown threats across the Caucasus, the Middle East and Europe. Notwithstanding near-universal relief that the proto-state is all but defeated, the exodus of thousands of foreign fighters signifies a period of extended disruption. Indeed, the Islamic State previously warned it is preparing for the 'long war' as it readies for its eventual loss of territory in Syria and Iraq.

The immediate goal of the majority of extremist movements remains limited to the national agenda, but the endurance of the jihadist diaspora and its pervasive online presence creates complex challenges for authorities globally. Sporadic attacks are simultaneously more difficult to detect and more terror-inducing, with the public fearing every large gathering is at risk.

As Jeh Johnson, former secretary of homeland security in the United States, has observed, we have moved from a world of terrorist-directed attacks to a world that also includes the threat of terrorist-inspired attacks, or attacks by those who live among us and self-radicalise, inspired by terrorist propaganda on the internet. Intelligence and law enforcement find terrorist-inspired attacks difficult to detect, and they could occur with little or no notice.

The contemporary security landscape is also characterised by extremist right-wing groups which openly espouse anti-immigration, national supremacist, or anti-Semitic ideologies. Such rhetoric is increasingly driving the political agenda in the U.S. and many European countries, fuelled by the recent tide of refugees from the Middle East.

The result of this ethno-nationalism, coupled with ongoing austerity in many industrialised countries, is the emergence of radical left-wing groups. Frequently self-styled as anti-fascist protesters, these groups include commercial, financial and law enforcement assets amongst their targets. Underpinning these political ideologies, especially right-wing populism, is 'fake news' distributed by robotic algorithms to pursue polarising political goals and disrupt mainstream media.

In fact, the ubiquity of digital devices – and users' insatiable appetite to engage online – has served to expose a whole generation to extremist messaging, be this jihadist videos, alt-right blogs, trolling networks or 'antifa' (anti-fascist) slogans. Furthermore, on the fringes of extremist movements there exists lone individuals who actively participate online but do not belong in any formal sense. These lone actors are unlikely to draw the attention of law enforcement, and it is often almost impossible to disrupt the malign actions that might result from their radicalisation. Motivations behind such attacks also tend to be personal and ambiguous, further complicating efforts by authorities to prevent incidents and to identify the radicalising forces.

Another feature of the contemporary security landscape is the geographical and political diversification of targets. In particular, the shift in attacks by well-financed, organised jihadist cells to homegrown perpetrators has widened the terrorism nexus from global cities and seats of power to include lower-profile urban conurbations and towns. Local sites familiar to the adversary such as the workplace, transport hubs, commercial sites and industry facilities have all become potential targets

Introduction to Radicalisation

Despite many large organisations employing advanced physical security protections, the threat of terrorist infiltration remains a pressing concern for security managers, particularly given the now globalised, digital process of radicalisation. Although the 'insider threat' has always existed, in the information age lone individuals may be radicalised more easily and may take proactive steps to evade detection as they seek to harness their privileged insider access, authority and knowledge for malign purposes.

RADICALISATION

THE PROCESS THROUGH WHICH AN INDIVIDUAL OR A GROUP EVOLVES TOWARDS POLITICAL VIOLENCE OR FROM NON-VIOLENT TO VIOLENT EXTREMISM

'Radicalisation' itself is commonly defined as the process through which an individual or a group evolves towards political violence or from non-violent to violent extremism. In more generic terms, it is also described as "a change in beliefs, feelings and behaviours in directions that increasingly justify inter-group violence".[1]

Admittedly, there is no clear consensus on the legal and conceptual meaning of the term 'extremism', and experts consequently say that there is also no agreed upon definition of radicalisation.[2] This concept has, in fact, occasionally been contested in the literature. Those who have taken a sceptical or critical stance on radicalisation argue that one's understanding of it is often circumscribed to a limited number of cases, groups or ideologies that may oppose or threaten the status quo at a given moment in time. [3]

In a post-9/11 context, the term 'radicalisation' has most commonly been used in reference to jihadi terrorism, which has shaped the representation of this concept in today's media and political sphere. Processes of radicalisation manifest themselves in a very broad range of ideological, social or cultural environments, and researchers have studied them in a variety of contexts, ranging from nineteenth-century anarchism to twentieth-century sectarian conflicts in the Middle East.

Within the literature, radicalistion has been addressed from two different perspectives:

1. The Positivist Approach

On the one hand, experts in the fields of criminology, psychology and security studies tend to apply a positivist approach, assuming that radicalisation results from a combination of identifiable causes. This tradition pays particular attention to the grievances, identity issues, and feeling of injustice that underpin the evolution of a group or individual towards violent extremism. For example, social psychologists focus on the role of deindividuation, studying how one loses self-awareness to embrace a narrative that promotes inter-group violence. Criminologists alternatively postulate that a history of petty crime or criminality along with an experience of the prison system increase one's chance of becoming radicalised.[4] Some of the different factors that are thought to increase the risk of radicalisation are summarised in Figure 1.1.

1 Clark McCauley and Sophia Moskalenko, 'Mechanisms of Political Radicalization: Pathways Toward Terrorism' in Terrorism and Political Violence, 20 (2008), pp.415-433.

2 Alexander Meleagrou-Hitchens and Nick Kaderbhai, 'Research and Perspectives on Online Radicalisation, a Literature Review, 2006-2016' in VOX-Pol Network of Excellence (2017), pp. 1-94.

3 Arun Kundnani, The Muslim Are Coming: Islamophobia, Extremism, and the Domestic War on Terror (2014). London: Verso.

4 Rajan Basra, Peter Neumann and Claudia Brunner, Criminal Pasts, Terrorist Futures: European Jihadists and the New Crime-Terror Nexus. International Centre for the Study of Radicalisation (2016). Available online at: http://icsr.info/wp-content/uploads/2016/10/Criminal-Pasts-Terrorist-Futures.pdf [last accessed 06.04.2018]; Farhad Khosrokhavar, Prisons de France. Violence, Radicalisation, Déshumanisation: Surveillants et Détenus Parlent (2016). Paris: Robert Laffont.

In contrast, political scientists focus on understanding how violent radical groups operate as well as how they communicate their ideological message as a means of promoting radicalisation. In recent years, this type of research has been very active in documenting the emergence of a new kind of terrorist organisation that relies on global and leaderless networks.[5] As in the case of the so-called Islamic State (ISIS), such groups may be composed of a widespread community of both 'lone-wolf actors' and foreign recruits fighting in the conflict zone. This relatively new form of terrorism suggests that inter-group violence can spread far beyond the context of a local conflict. But most importantly, it indicates that violent radical groups can rely on innovative communication strategies to reach an increasingly diversified audience.

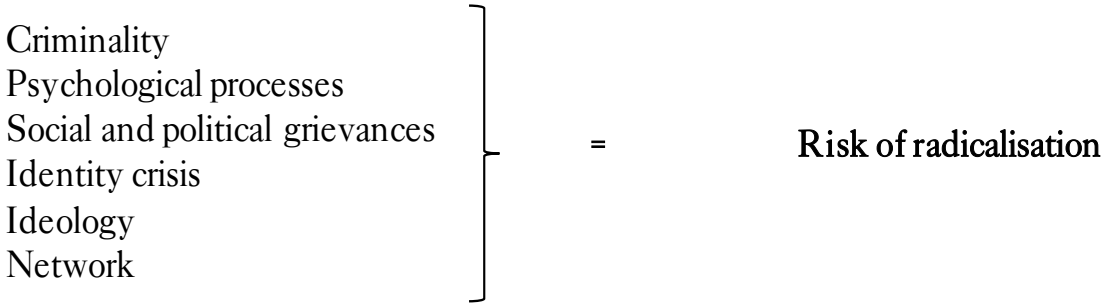


FIGURE 1.1: POSITIVIST APPROACH: POTENTIAL FACTORS OF RADICALISATION.

Researching the cases of ISIS's foreign recruits and supporters provides evidence to the idea that gender, education, religion and socioeconomic status are not consistently significant factors of radicalisation. Indeed, in the early 2000s experts had already argued there was no significant relationship between poverty and radicalisation.[6] They observed that terrorist groups' affiliates appeared to have secondary or higher levels of education, and that women and children were just as likely as men to engage in violent extremism.[7] More recently, the work of Bouzar and Rollie Flynn even suggests that ideology itself might play a marginal role in the radicalisation process – instead linking it to anyone who is disillusioned with society or their own life in some way.[8]

Amongst social scientists there is a general consensus that a crisis of identity is a central pre-cursor to radicalisation. Experiences of marginalisation and feelings of exclusion make potential recruits more vulnerable to radical groups' propagandists. In a context of loneliness and insecurity, individuals may uphold the identity of a group as a form of psychological shield and endorse this artificial identity to the extreme. For example, anthropologists have observed that a high proportion of young would-be ISIS foreign fighters were grieving the death of a family member prior to their radicalisation.[9] Many female recruits happen to have been victims of rape, which induced feelings of humiliation and a strong desire for revenge and redemption.[10] In this context, the social networks amongst which these vulnerable individuals interact both physically and online are also believed to be key determinants. A significant number of young recruits proved to have joined a movement because they were following their peers or a person whom they regarded as a particularly charismatic authority figure.

5 Marc Sageman, Leaderless Jihad: Terror Networks in the Twenty-First Century (2008). Philadelphia: University of Pennsylvania Press.
6 Alan Kreuger, What Makes a Terrorist? Economics and the Roots of Terrorism (2007). Princeton: Princeton University Press; James Piazza, 'Poverty and terrorism: a hypothesis in search of evidence' (2004) in Stuart Gottlieb, ed. Debating Terrorism and Counterterrorism: Conflicting Perspectives on Causes, Contexts, and Responses. Washington, DC: CQ Press; Marc Sageman, Understanding Terror Networks (2004). Philadelphia: University of Pennsylvania Press.
7 Alan Krueger and Jitka Maleckova ,'Education, Poverty and Terrorism: Is There A Causal Connection?' (2003) in Journal of Economic Perspectives, 17 (4), pp. 119-144; Mia Bloom, Bombshell: Women and Terrorism (2011). Philadelphia: University of Pennsylvania Press.
8 Dounia Bouzar and Carol Rollie Flynn, 'ISIS Recruiting: It's Not (Just) Ideological' in Foreign Policy Research Institute (2017). Available online at: https://www.fpri.org/article/2017/09/isis-recruiting-not-just-ideological/ [last accessed 06.04.2018].
9 Dounia Bouzar, La Vie Après Daesh (2015). Paris: Les Editions de L'Atelier.
10 Mia Bloom, Bombshell: Women and Terrorism (2011). Philadelphia: University of Pennsylvania Press.

Considering the above, members of law enforcement, governments and agencies working on Countering Violent Extremism (CVE) and Preventing Violent Extremism (PVE) initiatives have developed different criteria of behavioural changes when raising awareness about radicalisation. Amongst others, campaigns launched by the UK Home Office list the following potential signs of radicalisation:[11]

- Asking 'inappropriate' questions
- Becoming detached or withdrawn
- Signs of stress
- Quick to anger
- Isolation from friends and community
- Association with known radicals
- Attending rallies for extremist causes
- Advocating criminal or violent behaviour
- Exhibiting erratic behaviour including paranoia or delusion
- Speaking about revenge
- Displaying hatred or intolerance of other people/communities because they are different
- Feeling persecuted
- Refusing to listen to different points of view
- Embracing conspiracy theories
- Distancing oneself from old friends
- Sympathetic to extremist ideologies and groups
- Being secretive and reluctant to discuss whereabouts
- Accessing extremist online content

2. The Constructivist Approach

In opposition to the literature cited previously, there is an alternative school of thought that does believe there are consistent and observable radicalisation traits against which effective preventative measures can be implemented (summarised in Figure 1.2). Sociologists and political scientists within this group also argue that the debate on radicalisation feeds into inter-group violence by creating a disproportionate perception of threat and indirectly increasing identity issues by conveying mutual misrepresentations between the members of a so-called 'in-group' and an 'out-group'.[12] In other words, raising awareness about certain forms of radicalisation may increase the fear of – what in this context has been labelled as – 'the other' and create more grounds for inter-groups conflicts. Research demonstrates that this, for instance, is very likely to affect the way issues such as migration, multiculturalism and national identity are being debated in the post-2001 era.[13]

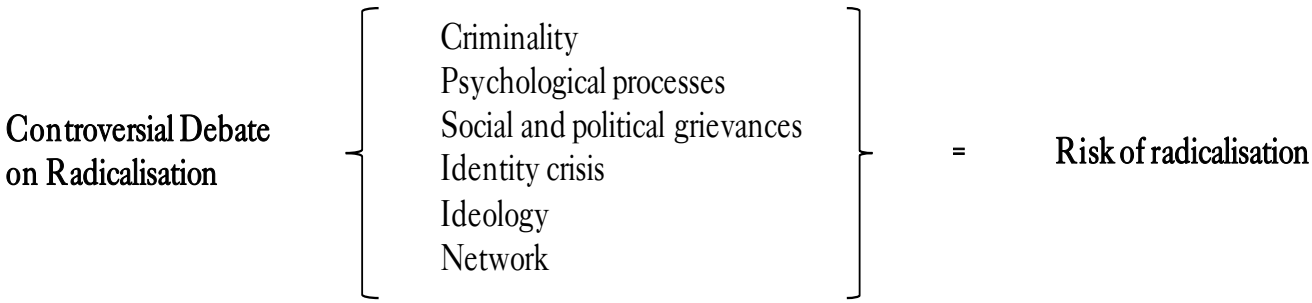


FIGURE 1.2: THE CONSTRUCTIVIST APPROACH – THE CRITICAL APPROACH OF RADICALISATION.

11 The Educate Against Hate and Refugee at Home campaigns jointly launched by the UK Home Office and Department for Education. See for example Laura Curtis, 'Internal Report on Radicalisation Prevention Strategies of the UK Government' (2017). Available online at: https://www.refugeesathome.org/files/PREVENT.pdf [last accessed 13.09.2018].

12 Bertjan Doosje, Annemarie Loseman and Kees Van den Bos, 'Determinants of the radicalization process of islamic youth in the Netherlands. Personal Uncertainty, perceived injustice and perceived group threat' (2013) in Journal of Social Issues, 69, pp. 586–604; Arun Kundnani, The Muslim Are Coming: Islamophobia, Extremism, and the Domestic War on Terror (2014). London: Verso; Shana Kushner Gadarian, 'The Politics of Threat: How Terrorism News Shapes Foreign Policy Attitudes' (2010) in The Journal of Politics, 72 (2), pp. 469-483.

13 Bertjan Doosje, Anja Zimmerman, Bearte Kupper, Andreas Zick, and Roel Meertens, 'Terrorist Threat and Perceived Islamic Support for Terrorist Attacks as Predictors of Personal and Institutional out-group Discrimination and Support for Anti-Immigration Policies – Evidence from 9 European Countries' (2009) in Revue Internationale de Psychologie Sociale 22, pp. 203-233.

In an organisational context, there is a risk that stereotypical representations of the radicalisation threat could result in internal prejudices and discrimination against certain staff. In turn, this could serve to increase the risk of radicalisation whilst also undermining the development of a robust security culture amongst the entire workforce. Consequently, institutions should take a nuanced approach when assessing the radicalisation risk, and implement appropriate preventative measures. These issues are explored in detail throughout the case studies contained within this handbook.

Overview of Preventative Measures

In a nuclear security context, preventative measures typically refer to systems and processes that serve to deter, preclude or defeat a potential internal adversary before they are able to initiate a malicious act.[1] As such, they are applicable both to current employees and individuals applying for access. Measures can include both pre-employment vetting and continuing behavioural observation and testing once employed. In particular, sensitive industries may also include certain oversight mechanisms and restrictions following the cessation of employment. Other preventative security measures include limiting individuals' access, authority and knowledge when it comes to both physical areas and information systems.

PREVENTATIVE MEASURES

SYSTEMS AND PROCESSES THAT SERVE TO DETER, PRECLUDE OR DEFEAT A POTENTIAL INTERNAL ADVERSARY BEFORE THEY ARE ABLE TO INITIATE A MALICIOUS ACT

The use of preventative measures may vary considerably across facilities and from country to country. Typically, a graded approach will be taken where both the threat level and potential consequence of a malicious act will be considered when deciding what security measures should be employed.[2] Given that many preventative measures are focused on assessing an individual's integrity, honesty and reliability, and on identifying potential undesirable personal characteristics or traits, their use can be controversial and at odds with broader national cultural values. This may limit the use of preventative measures in some countries. At an organisational level, the implementation of certain preventative measures such as behavioural observation and reporting can be challenging. This security measure will only be effective if all staff members are trained in what to look for, are vigilant and feel sufficiently empowered and protected by management to report aberrant behaviours on the part of their colleagues. It is a challenge to develop this type of security culture in any organisation as highlighted by the 2016 report published by the United States Department of Energy, which emphasised the need to strengthen protection for whistleblowers within their nuclear sector.[3] The case studies in this handbook serve to demonstrate further how preventative measures will be ineffective against insiders unless they are carefully implemented.

1 International Atomic Energy Agency, 'Preventive and Protective Measures against Insider Threats' (2008), IAEA Nuclear Security Series, No. 8. Available online at: https://www-pub.iaea.org/MTCD/Publications/PDF/ Pub1359_web.pdf [last accessed 13.09.2018] .

2 International Atomic Energy Agency, 'The Physical Protection of Nuclear Material and Nuclear Facilities' (1999), IAEA Nuclear Security Series No. 27-G (or 225, Revision 5). Available online at: https://www-pub. iaea.org/MTCD/Publications/PDF/PUB1760_web.pdf [last accessed 13.09.2018]

3 'Whistleblower Protections Need Strengthening' (2016), U.S. Department of Energy, GAO-16-618. Available online at: https://www.gao.gov/products/GAO-16-618 [last accessed 13.09.2018].

Insider Threats in the U.S. Military

Introduction

The military can present a challenging working environment, which in some cases can promote behaviours that may increase the risk of insider acts. Recruits can be exposed to stress, trauma and psychological distress, as well as heightened threat perception leading to 'strong identification with the 'in-group' and 'greater anxiety in inter-group interactions'.[14] In an interview with Stanford University News service, political scientist and security expert Scott Sagan emphasised the fact that 'insider threats are ubiquitous [...] in critical national security organisations', highlighting the U.S. military, stating that 'each of [its] services [had] suffered [...] from having a spy, a dangerous leaker of secrets or a terrorist within the ranks'.[15]

> **INSIDERS ARE A SIGNIFICANT ISSUE IN MILITARY ORGANISATIONS WORLDWIDE**

In order to understand what makes the military vulnerable to insider threats, this section explores three cases involving both serving officers and a former officer working as a contractor. All three cases are drawn from incidences involving the U.S. military. The focus on the United States is due to the rich body of publicly available information on insider incidents that can be drawn upon. However, it is clear that insiders are a significant issue in military organisations worldwide. The three cases selected involve attacks by violent insiders and the theft of sensitive information. They showcase a range of environmental factors that might serve as a trigger for insider actions, as well organisational issues that may lead to red flags regarding behavioural change and potential signs of radicalisation being missed.

14 Walter Stephan and Lausanne Renfro, 'The Role of Threat in Intergroup Relations' (2002) in Diane M. Mackie and Eliot R. Smith (eds.) Intergroup emotions and the social self: Prejudice reconceptualized as diverentiated reactions to outgroups. New York, PA: Psychology Press.

15 Clifton, B. Parker, 'Insider threats often go undetected in high-security organizations, Stanford scholar finds' (Stanford News Service, 22 June 2017). Available online at: https://news.stanford.edu/press-releases/2017/06/22/insider-threats-en-go-undetected/ [last accessed 10.08.2018].

Case Study 1: Attack at United States Military Base, Kuwait

Perpetrator Profile

Mark Fidel Kools had a difficult childhood, beginning with the incarceration of his father. While in prison his father was introduced to the Nation of Islam (NOI) and upon his release he converted family to Islam, changing Mark Fidel Kools' name to Hasan Akbar. Akbar's parents soon separated, but his mother remarried another NOI member, William Mohammed Bilal. Bilal allegedly sexually abused Akbar's sister and was arrested in 2003 for the possession of an illegal weapon. Given this prolonged period of instability, it is perhaps not surprising that at the age of fourteen, Akbar was diagnosed with depression and adjustment disorder.

In 1997, Akbar graduated from the University of California with a Bachelor's degree in aeronautical and mechanical engineering, which had taken him nine years to complete. In 2002, he joined the Army in order to repay his student debt, despite the fact that, as it appeared from the evidences later presented at his trial, his engagement in the U.S. military already conflicted with his ideological views. In 1993, Akbar had written in his personal diary that he did not like the military, and that he considered himself 'anti-government'.

Once enlisted, Akbar showed poor performance in the Reserve Officers' Training Corps (ROTC) programme. He was later appointed to the 326th Engineering Battalion at the rank of sergeant, despite most of his fellow recruits completing the ROTC with the higher rank of lieutenant. He was subsequently dismissed from his position as squad leader to a more menial position within his unit. Akbar had been occasionally disciplined for insubordination and retrospectively, following the attack, his colleagues described him as isolated and occasionally 'talking to himself'.[16] Despite his confrontational behaviour and history of depression, Akbar was assigned to supervise a unit clearing landmines, and was deployed to Kuwait in 2003 in preparation of the U.S. military intervention in Iraq.

Incident Summary

Over the months preceding the attack, Akbar reported to his parents that he had suffered harassment from white supremacist military recruits within his unit. He expressed his concern at the thought of being deployed in the Middle East, suggesting that this contradicted his religious beliefs and would cause tensions with members of his battalion. A month before the attack, Akbar stated that he would be forced to decide between 'killing [his] Muslim brothers fighting for Saddam Hussein or [his] battle buddies'.[17] Akbar committed the attack on the night of 22nd March 2003 as the 101st Airborne Division was preparing to move into Iraq and launch 'Operation Iraqi Freedom'. The attack took place at Camp Pennsylvania, located 25 miles from the Iraqi border.[18] An Air Force Major was killed by a grenade, an Army Captain was shot in the back, and fourteen other soldiers were wounded from grenade shrapnel.

16 Madeleine Gruen, 'Backgrounder: Sgt. Hasan Akbar' (January 2010), NEFA Foundation. Available online at: https://www.cia.gov/library/abbottabad-compound/16/165FA03E9D57C37C831563E53C4A8F97_NEFA_-_Backgrounder_-__Sgt._Hasan_Akbar_and_the_March_2003_Kuwait_Attack.pdf [last accessed 10.08.2018].

17 Ibid.

18 Brett Barrouquere, 'Appeal for Soldier Convicted in '03 Grenade Attack' (August 2014). Available online at: https://www.military.com/daily-news/2014/08/27/appeal-for-soldier-convicted-in-03-grenade-attack.html [last accessed 10.08.2018]; United States Court of Appeals for the Armed Forces, 'United States Versus Hasan Akbar (August 2015), No. 13-7001/AR. Available online at: http://www.armfor.uscourts.gov/newcaaf/ opinions/2014SepTerm/137001.pdf [last accessed 10.08.2018].

While most of his brigade was sleeping, Akbar shut off the generator for the outdoor lighting to the tent area. According to the U.S. court report, he threw a first grenade at a tent, where three officers (a Colonel, a Command Sergeant Major and a brigade Executive Officer) were sleeping. When the brigade Executive Officer emerged from the tent, Akbar fired at him with his M-4 rifle, seriously injuring him. He subsequently threw two fragmentation grenades into a second tent, where several officers and interpreters were sleeping. One of the targets was killed from eighty-three shrapnel wounds. Akbar then threw another fragmentation grenade into a third tent, where sixteen officers were located, and shot one of them in the back as he attempted to leave. In response, Akbar was stopped by an officer from brigade S-2, who tackled him to the ground. In April 2005, he was convicted of premeditated murder and attempted murder by a military jury and was sentenced to death. In 2015, the highest military court affirmed the conviction and death sentence after appeal.[19]

Preventative Measures and Security Systems

Based on available open source information, it is not clear as to whether Akbar had disclosed information regarding his debts and/or history of mental illness to his army recruiters in 2002. However, his diary later revealed that he was contemplating the thought of harming fellow U.S. servicemen that same year.[20]

The facts presented by both the defence and the prosecution at the 2005 trial indicated that Akbar had shown many signs of distress including depression, insomnia and paranoia. He had been reprimanded for insubordination and he was later described as being lonely and isolated. Akbar's relatives also reported that he had filed a complaint stating he suffered from religious and racial abuse from members of his own unit. However, his superiors did not conduct a follow-up investigation. However, it is only once he was enrolled in the military that his behaviour became visibly confrontational. This indicates that a successful approach to the prevention of terrorist insider threat requires monitoring not only individuals' personal trajectories, but also complex social dynamics, such as inter-group relations.

Broader Issues

Certain aspects of this case led commentators to consider the possibility that racial, religious and other ideological conflicts might occur in the ranks of the U.S. military. For instance, Madeleine Gruen, Senior Analyst for the Nine Eleven Finding Answers Foundation (NEFA) noted that 'it is possible that White supremacist sympathizers in the military provoke already unstable minority soldiers to violent action. Their strategy is to exacerbate racial tensions in order to cause the tipping point that will ultimately lead to an all out race war'. [21]

Furthermore, the case of Hasan Akbar and others also contributed to the broader debate on the conditions of Muslim recruits in the post-9/11 U.S. military. Between 2010 and 2011, Muslim-American soldier Zachari Klawonn, who became Liaison Officer for the Military Religious Freedom Foundation, gave several interviews in which he denounced abuse and discrimination against Muslim-American military recruits. Klawonn also reported,

19 Michael Doyle, 'Military court upholds death sentence in 2003 'fragging' case' (August 2015), McClatchy DC Bureau. Available online at: https://www.mcclatchydc.com/news/crime/article31627586.html [last accessed 10.08.2018].

20 Brett Barrouquere, 'Military court weighs fate of condemned soldier for 101st Airborne' (November 2014) in Tenessean. Available online at: https://eu.tennessean.com/story/news/local/2014/11/18/military-court-weighs-fate-condemned-soldier-st-airborne/19247853/ [last accessed 10.08.2018].

21 Madeleine Gruen, 'Backgrounder: Sgt. Hasan Akbar' (January 2010), NEFA Foundation. Available online at: https://www.cia.gov/library/abbottabad-compound/16/165FA03E9D57C37C831563E53C4A8F97_NEFA_-_Backgrounder_-__Sgt._Hasan_Akbar_and_the_March_2003_Kuwait_Attack.pdf [last accessed 10.08.2018].

as in the case of Akbar, that his complaints had never been processed by his hierarchy. The issues he raised suggested that although the military is commonly perceived as an environment of successful social cohesion that promotes 'loyalty and camaraderie', soldiers can occasionally be ostracised for belonging to a stigmatised minority.[22] Experts in the field of social psychology and prejudice argue that this process, which may result into different forms of inter-group conflicts or identity crises, is even more likely to occur when subjects experience a high perception of threat:

> Strong identification with the ingroup should be associated with threat because people who identify with their ingroup are likely to be more concerned about losses in power and having to change their values and beliefs. They are also likely to feel greater anxiety in intergroup interactions, and the sharp distinction they draw between groups and their desire to view the ingroup positively may lead them to negatively stereotype outgroups.[23]

On the eve of the Iraq War, threat perception, which is relatively high in the military, increased amongst U.S. Armed Forces recruits.[24] Simultaneously, Muslim communities found themselves at the centre of media attention in the global climate of insecurity introduced by the so-called War on Terror. This in itself does not suffice to explain why a few individuals like Akbar evolved from cognitive (thoughts, beliefs, feelings) to behavioural (taking action on these) radicalisation[25]. However, it shows that a favourable environment for intergroup conflicts can act in conjunction with other parameters, such as trauma, depression or psychological distress. In this particular case, the history of mental illness coupled with the NOI politicised perspective on religious and racial identity potentially made Akbar more vulnerable to radicalisation.

22 Manuel Roig-Franzia, 'Army Soldier Is Convicted In Attack on Fellow Troops' (April 2005) in Washington Post. Available online at: http://www.washingtonpost.com/wp-dyn/articles/A7210-2005Apr21.html [last accessed 10.08.2018].

23 Walter G. Stephan and Lausanne Renfro, 'The Role of Threat in Intergroup Relations' (2002) in Diane M. Mackie and Eliot R. Smith (eds.) From Prejudice to Intergroup Emotions: Differentiated Reactions to Social Groups. New York, PA: Psychology Press.

24 Luis R. Perez, Threat Perception, Non-State Actors, and U.S. Military Intervention after 9/11 (2016). Thesis submitted to the faculty of the Virginia Polytechnic Institute and State University in partial fulfillment of the requirements for the degree of Master of Arts In Political Science. Available online at: https://vtechworks. lib.vt.edu/bitstream/handle/10919/73306/Perez_LR_T_2016.pdf?sequence=1 [last accessed 13.09.2018].

25 See for example Miguel Peco Yeste 'A Cognitive-Behavioral Approach to Violent Radicalization, Based on a Real Case' (2014) in Psicologia Politica, No. 49, pp. 7-26.

Case Study 2: Attack at Military Naval Yard, United States

Perpetrator Profile

Aaron Alexis was a Buddhist convert and U.S. Navy Veteran who worked for the Washington Navy Yard as a military recruit, and then a contractor from 2007 to 2012. Prior to taking up these positions, Alexis had been involved in a number of petty crime incidents. However, these did not alarm his Navy recruiters. A police investigation was opened in 2004 after Alexis was first arrested in Seattle for 'malicious mischief'.[26] A witness reported that he had shot the tires of a neighbour's car, which Alexis admitted during his interrogation. At the time, Alexis and his father both claimed that he had been suffering from 'PTSD' and 'anger management problems' ever since he had joined the 9/11 rescue efforts in 2001. The U.S. 'Oversight and Government Reform' Committee, who re-examined the case, was unable to confirm these claims.[27] According to the criminal report, the incident was referred to Seattle Municipal Court in June 2004 for charges of unlawful discharge of a firearm and property damage. However, the court spokesperson retrospectively stated that the administration had never received the case. Consequently, charges were dropped when Alexis was received in court on July 2004.

Two years later, Alexis was identified by the Washington Police as the 'involved person' after tires were found slashed on five of his neighbours' vehicles. No arrest was made in this case.[28] He was left with several unpaid student loans after quitting university, and had accumulated traffic tickets, most of which were left unpaid when he enlisted in the Navy in 2007. When meeting with Navy recruiters, Alexis claimed he had no history of criminal activity and indebtedness. As per the procedure, the Office of Personnel Management conducted the required 'Entrance National Agency Check', which alerted the recruiters about the debts. However, the Naval Recruiting District (NRD) did not check police records as Alexis had not spontaneously reported his history of criminal activity. As part of the recruitment process, Alexis completed the Armed Services Vocational Aptitude Battery with a score of 78 (above the 2007 average of 63.08), which likely helped to convince the NRD that he was suitable for service. In addition, the medical screening did not reveal any concerns of mental illness, and Alexis denied suffering from any form of psychological distress in his medical document. As a result, he was considered suitable for recruitment, and the Navy only notified his squadron that he had a negative credit history. Alexis was granted a secret level clearance. He then served as a full-time reservist until 2011, only reaching the rank of petty officer, third class.

Incidences continued to occur after he started work at the Washington Navy Yard. In 2008, he was arrested and disciplined for being absent from the Navy without leave, and later that year jailed on charges of disorderly conduct after breaking furniture in a night club. These charges were dropped, although it was less than a year before Alexis was once again disciplined and almost dismissed for being drunk on duty. In 2010, he shot a gun in his apartment and was again arrested, although the charges were later dropped, with Alexis claiming his gun discharged inadvertently while he was cleaning it. During this time

26 U.S. House of Representatives, Committee on Oversight and Government Reform, Slipping Through the Cracks: How the D.C. Navy Yard Shooting Exposes Flaws in the Federal Security Clearance Process (2014), Staff Report of the 113th Congress, p.4.

27 Ibid.

28 Admiral John M. Richardson 'Investigation into the Fatal Shooting Incident at the Washington Navy Yard on 16 September 2013 and Associated Security, Personnel, and Contracting Policies and Practices' (November 2013). Department of the Navy. Available online at: http://archive.defense.gov/pubs/Navy-Investigation-into-the-WNY-Shooting_final-report.pdf [last accessed 10.08.2018].

period Alexis manifested multiple symptoms typically of paranoia. The subsequent FBI investigation following the attack on the naval yard revealed that he suffered from severe delusions, heard voices, and believed he was controlled by electromagnetic waves. His mental and emotional condition was retrospectively described as visibly unstable.

In 2012, Alexis received an honourable discharge from the military, thereby retaining his security clearance for an additional ten years and consequently remaining employable by military subcontractors and others. At the time of the shooting, Alexis was employed by an I.T. subcontractor called 'The Experts', providing intranet networks to the U.S. Navy.

Incident Summary

On 4th August 2013, as Alexis was travelling on assignment to a naval station in Rhode Island, he called his project coordinator at 'the Experts' to say that an individual seating next to him was making fun of him, and that he was feeling angry. The project coordinator reassured Alexis over the phone and notified 'The Experts' program team of the incident the next day. On 5th August, during his stay in Rhode Island, Alexis called the company's travel coordinator to complain about noises in his room. On 6th August, the Naval Station Newport police received phone calls from the clerk of the local hotel where Alexis was staying, as well as from 'the Experts' travel coordinator, suggesting that Alexis should be monitored and that his behaviour had led them to believe that he might cause harm to others. Officers from the Naval Station Newport police visited Alexis. During the interaction, he claimed that a chip had been placed in his head and that he it had been designed to send microwave signals through his body.

Alexis was visibly suffering from an episode of paranoia, but the police officers decided that he did not represent a threat. He was therefore not put in custody and was not even advised to seek immediate treatment. 'The Experts' travel coordinator reported his behaviour to the management team and Alexis was notified, on that same evening, that he was expected to come back to Fort Worth for his assignment at Newport was now cancelled. The following day Alexis complained again to the local police and his shift deployment supervisor about being followed and persecuted . Meanwhile, 'The Experts' initiated administrative procedures to ensure that Alexis would no longer be allowed to access the Naval Undersea Warfare Center as initially required for his assignment, and a debrief was issued to establish that Alexis would also no longer need access to classified information. This internal document, however, did however not comment on the reliability of Alexis as an individual. Simultaneously, 'The Experts' Human Resources initiated an internal investigation, seeking legal counsel. They liaised with Rhode Island local police, although no report was filed. On 9th August, in spite of the alarming testimonies of colleagues and family members, the management team decided that 'the information collected about Alexis was based on rumor and innuendo, and therefore a report to the government should not be made, since doing so may infringe on Alexis' privacy rights'.[29] His access to classified information was restored and Alexis was allowed to rest until his next assignment, which was scheduled for 12th August. He then completed four assignments with no signs of unusual behaviour between mid-August and early September. The investigation later revealed that he asked for medical advice for insomnia in a Veteran's treatment facility and showed signs of paranoia when interacting with civilians between 23rd August and 1st September. Alexis had been asked to work at the Washington Navy Yard for the week starting on 9th September 2013.

29 Admiral John M. Richardson 'Investigation into the Fatal Shooting Incident at the Washington Navy Yard on 16 September 2013 and Associated Security, Personnel, and Contracting Policies and Practices' (November 2013), Department of the Navy. Available online at: http://archive.defense.gov/pubs/Navy-Investigation-into-the-WNY-Shooting_final-report.pdf [last accessed 10.08.2018].

On 14th September, Alexis purchased a Remington-870 and a 12-gauge shotgun in Virginia. In the morning of 16th September, he entered Washington Navy Yard at 07:44 using his common access card, which was given to military or civilian personnel as well as contractors. He parked his car and entered the closest building (building 197) using an electronic badge (valid temporary building pass). Alexis was carrying the shotgun along with ammunition in a bag. He loaded the gun in a bathroom located on the 4th floor, exited the bathroom, and began shooting at people. The Metropolitan Police Department were notified within a few minutes and Alexis was shot and killed by law enforcement officers. He had killed twelve people.

Preventative Measures

In response to the infamous mass shooting committed by Fort Hood soldier in 2009, then-Secretary of Defense Robert Gates had established an Independent Review within the U.S. Department of Defense designed to improve force protection at military bases. A report containing 47 recommendations was issued in 2010.[30] It called for greater awareness of behavioural indicators related to radicalisation and for the consolidation of a criminal investigation and law enforcement database within the Department of Defense. However, these preventive measures did not anticipate the risks of insider threat in relation to the 900,000 civilian contractors working for the Defense Department.

In 2013, one of the largest security providers in charge of vetting procedures for U.S. government contractors was USIS (U.S. Investigations Services). USIS carried out 65% of the background investigations conducted by private security providers for the U.S. Office of Personal Management (OPM) and had vetted Edward Snowden (see Case Study 3). As part of the subsequent investigation, USIS revealed that it had conducted a background check of Aaron Alexis in 2007, at the time of his enlistment. His security clearance had subsequently been granted, despite his arrest in 2004. The government announced that the company was under criminal investigation related to the incident and USIS agreed to forego its right to collect payment of $30 million from the OPM in 2015. In addition, OPM announced in September 2014 that it would not renew its contracts with USIS.

The subcontractor company 'The Experts' confirmed Alexis' security clearance with the Defense Department in September 2012 and in June 2013 after Alexis returned from a short leave of absence. However, his vetting was never rerun since he was granted his secret-level security clearance as a reservist in 2008. No additional background checks were conducted and the OPM was never informed by his employers, colleagues, the police or others that Alexis had exhibited visible signs of psychological instability.

This incident revealed a concerning lack of communication between the three agencies in charge of monitoring Alexis throughout his career. The Navy did not spontaneously report charges of disorderly conduct to USIS when Alexis was offered a ten-year security clearance as part of his honourable discharge. It had also failed to identify his psychological instability during the recruitment process, consequently exposing him through his employment to a level of stress, pressure and psychological tension that he may not have been able to process as well as the average recruit. USIS had not been proactive in seeking additional information before reissuing his security clearance. Finally, the subcontracting company, 'The Experts', at which he worked prior to the shooting, did not inform USIS that he was exhibiting clear signs of pathological behaviour.

30 Nancy A. Youssef and Marc Seibel 'Fort Hood shooting revealed multiple military security lapses' (August 2012), McClatchy DC Bureau. Available online at: https://www.mcclatchydc.com/news/politics-government/article24590842.html [last accessed 10.08.2018]; Department of Defense Science Board, 'Task Force Report: Predicting Violent Behavior' (August 2012). Available online at: https://www.acq.osd.mil/ dsb/reports/2010s/PredictingViolentBehavior.pdf [last accessed 10.08.2018].

Broader Issues

This case has attempted to challenge the popular understanding of radicalisation, identifying alternative factors to be considered beyond the role of radical ideology or terrorism networks' recruitment. As such, this case reminds us that the use of violence can be explained by a combination of environmental and psychological parameters that operate in the absence of a specific ideological framework for cognitive radicalisation.

According to a 2015 study, mental disorders are the most frequent diagnosis for veterans treated through the health care system provided by the U.S. Department of Veterans Affairs (VA Healthcare).[31] 56% of veterans evaluated suffered mental disorders, with a majority recorded as post-traumatic stress disorders (PTSD). It is also estimated that a significant proportion of veterans suffering from PTSD, amongst other mental disorders, do not seek treatment. Research indicates that, although having a mental disorder would disqualify a person from enlisting in the military, 25% of non-deployed U.S. military recruits suffer from conditions like schizophrenia, bipolar disorder, panic disorder or obsessive-compulsive disorder. Issuing security clearance to members of a population that are statistically at risk of mental health disorders, stress or trauma requires running updated security checks before, during and after employment. This involves developing a collaborative approach to the prevention of insider threats when more than one institution is involved in the monitoring of behavioural changes and possible signs of radicalisation.

This selection of cases shows that pathways of radicalisation are often determined by a combination of parameters. Individuals may be exposed to propagandist material or fall under the influence of a charismatic leader promoting a radical ideology. These external parameters are sometimes referred to as 'pull-factors' of radicalisation.[32] However, the fact that some individuals are receptive to these stimuli can only be explained from the perspective of what constitutes their environment and life experiences. This may relate to the socio-political context in which processes of radicalisation operate as well as to family history, mental health, or professional trajectory of the individual in question. Within this broader range of variables, one can identify different 'push-factors' of radicalisation that could be reduced by implementing a relevant preventative approach.

In the U.S. military, inter-group conflicts, stress, trauma, and psychological distress have proved to act as push factors of radicalisation that could easily be tackled when raising awareness about the risks of insider threat.

Suggested Discussion Points:

- Which push-factors and pull-factors of radicalisation can be identified for each of these three cases?
- What measures would help when raising concerns over responsibility and liability in relation to the prevention of terrorist insider threat?
- What does the case of Aaron Alexis say about the relationship between employers and external security providers such as USIS?
- What kind of preventive measures could help improve social cohesion in a context of high perception of threat?

31 U.S. Veterans Health Administration, 'Analysis of VA Health Care Utilization among Operation Enduring Freedom (OEF), Operation Iraqi Freedom (OIF), and Operation New Dawn (OND) Veterans' (January 2015). Available online at: https://www.publichealth.va.gov/docs/epidemiology/healthcare-utilization-report-fy2014-qtr4.pdf [last accessed 10.08.2018].

32 See Matteo Vergani, Ekin Ilbahar, Greg Barton & Muhammad Iqbal 'The Three Ps of Radicalization: Push, Pull and Personal. A Systematic Scoping Review of the Scientific Evidence about Radicalization Into Violent Extremism' (2018) in Studies in Conflict and Terrorism, Vol. 49, No. 9.

Case Study 3: Theft of classified information from United States Military

Perpetrator Profile

Chelsea Manning is a former U.S. army intelligence officer who was convicted in 2013 for violating the Espionage Act after the largest leak of classified material in U.S. history. Between 2010 and 2011, the whistleblowing site WikiLeaks generated an international outcry after publishing classified material provided by Manning. Whilst the material shed light on human rights abuses by the U.S. military, the disclosure was deemed a direct threat to national security. Manning received a 35-year sentence – the longest ever imposed under the Espionage Act – although this was later commuted in 2017.

Chelsea Manning, born Bradley Manning, endured a difficult childhood with alcoholic parents, and was later bullied as a teenager over her small stature and conflicted sexuality. These issues were later raised in court as part of her defence team's mitigation for the data breach. However, despite these challenges growing up, Manning excelled at school and developed advanced computer skills. At the age of thirteen, Manning's parents divorced and she moved from her childhood home in Oklahoma to Wales in the United Kingdom. With newfound freedom, she began to question the conservative, religious values that had informed her upbringing, and also became increasingly politically engaged. Yet after returning to the U.S., Manning ultimately dropped out of community college and took a series of low-paid jobs.

In 2007 at the age of 19, Manning enlisted in the army. At the time Manning told her friends she was motivated by a genuine desire to serve America, as well as the opportunity to gain a university education, even aspiring to pursue a doctorate in physics. She later confided to a superior that the decision to enlist was to resolve her struggles with gender identity. Manning began basic training in October 2007 at Fort Leonard Wood, Missouri. However, just six weeks into the course, Manning was moved to a discharge unit after it became apparent that she was neither mentally nor physically prepared for the army. Yet despite ongoing concerns by her superiors, and being subject to intense bullying, the plan to discharge Manning was reversed and it was decided that she would be trained as an I.T. intelligence analyst. The Iraq war was in its fourth year and the U.S. army was struggling to enlist and retain recruits.

Manning subsequently received intelligence training at Fort Huachuca in Arizona, where her situation improved. However, she was reprimanded for posting videos on YouTube about the army base. Whilst she did not disclose classified records, she revealed the rooms where sensitive information was being held. Yet despite this breach, Manning went on in August 2008 to receive a top-secret clearance. Now a fully-fledged I.T. intelligence analyst, Manning was stationed at Fort Drum, New York state. Nevertheless, she was still considered a 'liability' by senior officers and required to access mental health counselling. At Fort Drum, Manning had her first serious boyfriend, a Brandeis University student who introduced her to a community of I.T. students interested in simulated codebreaking and hacking. For the first time, Manning had found a social niche where she was accepted as openly gay and shared interests in social justice.

Even so, Manning still adhered to the army's 'don't ask, don't tell' policy whilst at camp. And whilst she may have been growing in confidence in her private life, questions were re-emerging about her suitability for military service. When her unit was dispatched to Iraq in 2009, Manning's superiors initially discussed putting her deployment on hold. Yet again, the pressure to find recruits for Iraq proved too great, and it was hurriedly concluded she was showing 'signs of improvement'.[33] Just a few months later, Manning was deployed to Iraq where she committed the largest data breach in U.S. history.

33 Madar, C. The Passion of Bradley Manning: The Story Behind the Wikileaks Whistleblower (2013). New York, Verso Books.

Incident Summary

In October 2009, Manning was deployed to Forward Operating Base Hammer, one of the most isolated posts in Iraq. According to soldiers who served alongside Manning, Hammer base was characterised by boredom and mistreatment, with non-commissioned officers routinely bullying their subordinates. Soldiers also openly turned to the SIPRNet classified intelligence network for 'entertainment', downloading military footage such as Apache helicopters gunning Iraqi civilians down. It was in this context that Manning became increasingly disturbed about U.S. operations in Iraq. Only a month into her new role in Iraq, Manning was promoted to the rank of specialist. However, her resentment was only amplified with her more active involvement in U.S. military operations. Above all, she took umbrage with the arrest of non-violent civilians, being aware that torture was taking place in Iraqi prison camps. During this period, Manning began logging into internet chat rooms devoted to Wikileaks.

In early 2010, Manning was granted leave to return to the U.S. for two weeks. Before she left the Iraqi base, she took the monumental decision to download almost every single report covering the Iraq and Afghanistan wars from the government's Combined Information Data Network Exchange. Manning allegedly did this in full view of her colleagues. One of the CD-RW discs where she compressed the data was labelled 'Lady Gaga'. She later transferred the data to her personal laptop, thereby violating the army's fundamental Oath of Enlistment. Once in the U.S., Manning attempted to establish a confidential line of communication with three publishing companies: the *New York Times*, *Washington Post* and *Politico*. However, these efforts floundered and, with her leave running out, Manning decided to send the classified material to the whistle-blowing website Wikileaks.

Back in Iraq, several weeks passed without Wikileaks confirming receipt, and Manning became anxious that the site had not received her files. With the Icelandic financial crisis unfolding, she decided to release another tranche of diplomatic cables to Wikileaks, this time relating to Iceland. Within hours, these cables were made public, indicating that Wikileaks had indeed received her previous material. Manning passed on additional files over the following months, including footage taken in 2007 of a U.S. helicopter gunning down Iraqi civilians and two Reuters staff. Entitled 'collateral murder', the helicopter footage was premiered in April 2010, placing it firmly in the public consciousness.

Around this time, Manning's relationship with her boyfriend in Boston ended, leaving her distraught. With her behaviour deteriorating, she was demoted from the rank of specialist to private first class. Legal investigators would later uncover reports of Manning engaging in violent outbursts during her Iraq deployment. In one episode, she allegedly struck a female superior. In another, her rifle was disabled over fears she was unfit to carry a functioning weapon. Yet remarkably, Manning was allowed to retain her security clearance.

In May 2010, Manning started confiding online to a former hacker, Adrian Lamo, who himself had been convicted for breaking into computing networks at Microsoft, Yahoo and the *New York Times*. After Manning confessed about the data leak, Lamo secretly informed the federal authorities. One of the issues that Manning discussed with Lamo was the lax security at the Hammer base. But the chat logs also reveal that Manning's motivations for the breach were deeply political, centred on exposing what she perceived as American exploitation of developing countries. According to Manning, if the public could 'see the truth' they could make informed decisions that 'might actually change something'.[34]

Days after Lamo reported the leak, Manning was arrested and repatriated to face a U.S. military trial. Amidst much publicity, Manning spent three years before her case was brought to trial with a spate of suicide attempts and long periods in solitary confinement. In 2013, she received a 35-year sentence, the longest ever punishment ever imposed for the leaking of classified material. Shortly after her internment, Manning requested gender reassignment treatment and in the following years transitioned into a woman.

34 Zetter, K. and Poulson, K., 'I can't believe what I'm confessing to you: The Wikileaks chats' (2010) in Wired. Available online at: https://www.wired.com/2010/06/wikileaks-chat/ [last accessed 14.09.2018].

In January 2017, just days before his presidency ended, Barack Obama took the decision to commute Manning's sentence. Obama stated that the 35-year sentence was 'very disproportionate relative to what other leakers have received'.[35] Manning's defence lawyer suggested the commutation sent out a positive message that bringing important information into the public domain was valued. The decision was heavily criticised by Republicans and incoming U.S. president Donald Trump.

On her release, Manning was the focus of massive media interest, although notably she remains subject to a suppression order preventing her from speaking about certain details of her conviction. Manning ran for the U.S. Senate in June 2018, a race she lost by a large margin to the incumbent Democrat. Apparently motivated by a desire to shake up establishment Democrats, she ran a grassroots campaign with a platform that included universal healthcare, closure of prisons and elimination of national borders.

Preventative Measures and Security Systems

Chelsea Manning is lauded in some circles as a hero for calling the U.S. to account for human rights abuses, whilst others call her a traitor for disclosing top military secrets and potentially putting lives at risk. Certainly, her actions had a monumental impact on exposing human rights abuses in Iraq and Afghanistan. The data breach also reverberated on virtually every U.S. diplomatic relationship after Wikileaks began publishing embassy cables in November 2010. The task here, however, is not to extricate value judgements about Manning's deeds but to assess the circumstances that enabled her to carry out the breach.

By all accounts, Manning was highly vulnerable – both physically and mentally – throughout her army career. She was the target of unrelenting bullying and ridicule, and was prone to emotional outbursts, some of which reportedly resulted in violence, screaming and incontinence. Yet not only did Manning remain enlisted, she went on to receive specialised training and was ultimately given access to highly confidential military material in a war context.

Manning's unsuitability for the army was detected just six weeks into her tenure when basic training officers recommended that she be discharged. Pressure to enlist and retain recruits likely led to the decision to reverse her discharge, with 2007 recruitment numbers being some of the lowest on record amidst unpopular wars in Iraq and Afghanistan. There was also an urgent need for I.T. intelligence analysts in Iraq, resulting in a lowering of recruitment and retention standards. An unnamed soldier recounted to *The Guardia*n:

> *In 2007 recruiting numbers were the lowest they had ever been. They were lowering recruitment standards like crazy. I mean, facial tattoos, too tall, too short, too fat, criminal record – it didn't matter. They even upped the age limit. You could be 42 years old and still enlist for basic training. It was take everybody you could get. Keep hold of everybody you can get.* [36]

The soldier further noted that the decision would have been signed off up the chain-of-command:

> *It went to the first sergeant and company captain. They signed off on it and the whole packet began. Physical doctors and mental health professionals failed on him. Then you have the cadres, the drill sergeants in the DU: they failed on him. The first sergeant and the company captain at the DU failed him. The judge advocate group that everyone in discharge had to go through, they failed him. That is a lot of people in a lot of offices.*

35 See for example 'President Obama Defends Commuting Chelsea Manning's Sentence in Final Press Conference' (2017) in Times. Available online at: http://time.com/4638194/president-obama-final-press-conference/ [last accessed 14.09.2018].

36 Guardian interview, 'Bradley Manning: fellow soldier recalls scared bullied kid' (May 2011) in The Guardian. Available online at: www.theguardian.com/world/2011/may/28/bradley-manning-video-transcript-wikileaks [last accessed 14.09.2018].

IN 2010

WHEN THE BREACH TOOK PLACE, TWO MILLION PEOPLE HAD ACCESS TO SIPRNET

The soldier then went onto discuss the issue of liability:

> *You can't get mad at the bull for wrecking the china shop when you have trapped the bull inside it. Bradley should never have been there. They had the opportunity to get rid of him and they didn't. That was October and November 2007. It is now 2011 and all we are hearing about is Bradley, Wikileaks, and he is the bad guy.*

These early red flags were followed by serious violations and calls for help throughout Manning's army career. As aforementioned, this included an incident in 2008 where she posted sensitive information about the Fort Huachuca base on YouTube. Leading up to Manning's Iraq deployment in 2009, officers repeatedly warned that she was mentally unstable. Even in Iraq, her seniors disabled her service rifle over fears she was unfit to carry a functioning weapon. Yet none of these warnings about Manning's behaviour were ever passed up the chain-of-command.

Parallels can be drawn to the case of Nidal Hassan who carried out the Fort Hood attack in 2009. The incident occurred a few months prior to Manning's data breach, amidst the same recruitment pressures for specialist roles. In Hassan's case, an acute shortage of psychiatrists in the U.S. Army's medical corps at the major and captain rank. In her detailed analysis of the case, Zegart argues that key organisational failures – namely decentralised structures, career incentives and general army culture – enabled Hassan's career progression in the face of overwhelming evidence of his ineptitude and extremist views.[37]

The Hassan and Manning cases also occurred whilst the U.S. military was engaged in protracted, distant wars in Iraq and Afghanistan. Despite the events of 9/11 highlighting the threat posed by insiders, the Department of Defense continued to view the protection of military resources as guarding against external dangers.[38] Insider threats relating to sensitive electronic data were even less understood.

Indeed, one of the issues that came to light during Manning's trial was the lax information security at the Hammer base in Iraq. Passwords to SIPRNet, the classified intelligence network from which Manning leaked data, were openly shared with sticky notes posted to computers. More generally, the trial exposed the weak security culture at the base. Night shifts were overseen by enlisted soldiers rather than (more senior) non-commissioned officers.[39] Soldiers openly accessed music and films from SIPRNet, the same system used for classified intelligence.

Characteristic of isolated posts, the weak security culture was partly a facet of the work community directly overlapping with the social community.[40] It was inconceivable to the soldiers at Hammer that an insider threat existed amongst colleagues, as they were fundamentally reliant on each other for their survival in a war zone. Moreover, information security was low on their priorities when physical security was at stake.

In 2010 when the breach took place, two million people had access to SIPRNet. This included the Iraqi military, which at the time contained rogue actors intent on expelling the occupying U.S. forces. What began in the post-9/11 era as an initiative to give the military, diplomatic, law enforcement and intelligence communities quicker and easier access to data had unintended consequences in reducing the security of sensitive information.

Notably, Manning's whistleblowing served to clear a path for Edward Snowden, a former CIA (Central Intelligence Agency) technical assistant who in 2013 leaked confidential details of U.S. and U.K. government surveillance programmes. These disclosures were

37 A. Zegart, 'The Fort Hood Terrorist Attack: An Organizational Postmortem of Army and FBI Deficiencies' (2016) in M. Bunn and S. Sagan (eds.) Insider Threats. Ithaca: Cornell University Press.
38 A. Zegart, 'The Fort Hood Terrorist Attack: An Organizational Postmortem of Army and FBI Deficiencies' (2016) in M. Bunn and S. Sagan (eds.) Insider Threats. Ithaca: Cornell University Press.
39 Madar, C. The Passion of Bradley Manning: The Story Behind the Wikileaks Whistleblower (2013). New York, Verso Books.
40 Khripunov, I. Nuclear Security Culture: The Case of Russia (2004). Center for International Trade and Security: University of Georgia.

considered the most significant breaches of the National Security Agency (NSA) in U.S. history. At the time, Snowden was working as a contracted network administer at NSA.

In May 2013, he claimed to be taking sick leave from his NSA role in Hawaii, but instead boarded a plane to Hong Kong where he leaked the surveillance data to media organisations. Facing charges under the U.S. Espionage Act, in June 2013 Snowden fled to Russia where he was granted asylum.

Snowden, like Manning, had displayed warning signs of an individual who was susceptible to misconduct. According to an unclassified summary of a report by the House Intelligence Committee, Snowden dropped out of high school and enlisted in the special forces, but was unable to complete the training. In the workplace, he had frequent conflicts with his managers. In the report's summary, Snowden was characterised as a 'disgruntled employee' and a 'serial exaggerator and fabricator'. It later emerged that the background checks conducted for his NSA contract work failed to investigate Snowden's work history after he claimed it was 'classified', and this was not checked with the CIA.[41]

During this period, around three million Americans held security clearance.[42] Yet until Manning and Snowden's breaches came to light, electronic data was not afforded stringent protections. In his biography of Manning, Chase Madar argues that the authorities simply did not recognise the need because of 'how thoroughly those with a security clearance had internalized the government's mindset'.[43] This meant that even relatively low-ranking officials such as Manning and Snowden were given access to highly confidential information.

Indeed, Manning had both 'top secret' and 'sensitive compartmentalized information' clearances, the latter on a need-to-know basis and requiring access codes. By the time Manning received top secret clearance in 2008, the military would have already spent significant resources on her training. Although concerns over her behaviour were repeatedly raised, Manning was disciplined rather than her access being restricted or removed. This suggests there was a disconnect between operational security and national security, with lack of controls over electronic data an easy loophole for an insider to exploit.

Another issue to have emerged from the Manning and Snowden cases is the 'over-classification' of U.S. government documents. According to the Information Security Oversight Office, the U.S. federal agency tasked with information security, 77 million documents were classified in 2010.[44] On an operational level, over-classification can lead to casual handling of documents with low value afforded to those that do require added protection. On a societal level, routinised secrecy can stifle debate about issues of public interest, ultimately undermining confidence in transparent, democratic government.

Suggested Discussion Points:

The Snowden and Manning cases taken together beg the question of how two otherwise anonymous functionaries in the U.S. military architecture could, within three years of one another, commit the largest breach of classified material in U.S. history. Despite unstable backgrounds and difficult relationships with their colleagues and superiors, they rose through the ranks to gain security clearances and have access to highly sensitive military data. Some possible questions for discussion are as follows:

- In the Chelsea Manning case, in what ways could the U.S. army have implemented preventative measures?
- How should governments deal with whistleblowers when they bring to light issues of public interest?
- How can the U.S. military share data effectively and efficiently with government agencies – including the diplomatic corps, law enforcement and intelligence – without the reducing the security of this data?

41 United States House of Representatives, Executive Summary of Review of the Unauthorized Disclosures of Former National Security Agency Contractor Edward Snowden' (September 2016). Available online at: https://intelligence.house.gov/uploadedfiles/hpsci_snowden_review_-_unclass_summary_-_final.pdf [last accessed 14.09.2018].

42 C. Madar, The Passion of Bradley Manning: The Story Behind the Wikileaks Whistleblower (2013). New York, Verso Books.

43 Ibid.

44 S. Shane, 'Complaint Seeks Punishment for Classification of Documents' (August 2011) in New York Times. Available online at: www.nytimes.com/2011/08/02/us/02secret.html [last accessed 14.09.2018].

Insider Incidents in the Russian Northern Fleet

Introduction

Presented here are two incidents from the post-Soviet Russian Northern Fleet that will serve to demonstrate the importance of preventative measures against insider threats within a nuclear context. While the first incident examined will present an archetypal insider theft of nuclear material motivated by economic circumstances, the second will present a violent attack seemingly instigated by poor conditions and failed mental health screening. When studied together, these cases present systemic failures in insider threat prevention that contributed to the high frequency of insider incidents in post-Soviet Russia.

1991–1994

AROUND 700 ATTEMPTED SALES OF STOLEN RUSSIAN NUCLEAR MATERIAL WERE UNCOVERED IN GERMANY

After the collapse of the Soviet Union in 1991, weak state institutions, poor economic conditions, the lack of functional social security structures and failing law enforcement agencies led to a large uptake in both petty and organised crime. These conditions frequently manifested in the post-Soviet nuclear sector as insider incidents where valuable materials of all types were stolen by workers to augment their wages.[45] According to Mozley, between 1991 and 1994 around 700 attempted sales of stolen Russian nuclear material were uncovered in Germany, half of which were thought to involve genuine material being sold.[46]

As Russia's economic crisis continued into the late 1990s, pay arrears remained a constant problem and violent munities and incidents within the armed forces were routinely reported.[47] The frequency, severity and widespread nature of these insider incidents indicate the widespread failure at insider threat prevention within post-Soviet nuclear facilities. While many of the conditions that led to the prevalence of insider nuclear threat incidents were at a systemic and national level, it is worth considering how they applied to individual qualitative case studies and what actions, if any, could have been taken to prevent them.

45 Rensselaer Lee, 'Nuclear Smuggling from the Former Soviet Union: Threats and Responses' (2001) in Bu.Edu. Available online at: https://www.bu.edu/globalbeat/nuclear/FPRI042701.html [last accessed 14.09.2018].
46 Robert Fred Mozley, The Politics And Technology Of Nuclear Proliferation (1998). Washington: University of Washington Press.
47 BBC News, 'Russian Sailor Dies In Sub Shoot-Out' (1998). Available online at: http://news.bbc.co.uk/_1/hi/world/europe/169653.stm [last accessed 14.09.2018].

Case Study 4: Theft of Enriched Uranium at Sevmorput Shipyard, Russia

Perpetrator Profiles

All three individuals reportedly involved in the theft of 4.5 kg of enriched uranium fuel from Sevmorput shipyard on 27th November 1993 were current or former Russian naval officers who served at the shipyard over the courses of their careers. Captain 2nd class Aleksei Tikhomirov, 35, was deputy chief engineer (with fifteen years of experience). His younger brother, senior lieutenant Dmitriy Tikhomirov, was the chief officer assigned to refuelling operations at the facility. Oleg Baranov was the third accomplice in the conspiracy. He was a former naval captain, retired to the reserve, and was unemployed at the time of the theft. Aleksei and Oleg had served together in the same team at Sevmorput for over ten years, establishing a close relationship. The final indictment on their case does not reveal any startling information about their political affiliations or mental states. None of the offenders appeared to have an unusual background and the indictment makes only cursory mention of their service careers. For instance, Oleg Baranov was 'positively' described as a competent and disciplined officer during his service with the design bureau. In contrast, Dmitriy Tikhomirov is cited as having a poor service record, noted for a lack of commendations and five disciplinary infractions.[48] While it is questionable as to whether Dmitriy should have been working in such a senior role in proximity to special nuclear material given his record, it clearly did not disqualify him from such work at the time of the incident.

In addition to none of the individuals having remarkable personality characteristics, they also lacked any prior involvement in crime or any criminal connections. This would become evident in reports following the heist, as while their theft was well executed, there was no prearranged buyer for the fuel and it had to be stored until a suitable contact could be established. Oleg reportedly later claimed that he had been approached by 'strangers' in May 1993 who had offered to pay $50,000 per kilogram of uranium. However, this does not seem credible, given their subsequent difficulty in selling the material.[49] The amateurish nature of their crime was further established after they were arrested, as they were reportedly highly repentant and assisted with the investigation.[50] For instance, Dmitriy immediately confessed his involvement and led investigators to where they had stored the fuel. Nevertheless, it is likely that they had heard rumours of organised criminal groups being interested in acquiring nuclear material. Mikhail Kulik, the military prosecutor who investigated this incident, claimed that gangs had actively investigated and probed the security of Russian nuclear sites in the hope of acquiring uranium as an 'assassination weapon'.[51] Rather than any prior criminal expertise, it appears that their experience with the Russian navy clearly enabled their theft. Dmitriy's knowledge of the physical processes in handling of fresh fuel as well as his observation that security at the site was lax was likely the key enabling factor for the theft. Dmitriy reportedly extensively briefed his brother on how to conduct the heist.

The primary motivation for the participants appears to have been economic as their intention was always to sell the stolen fuel. It has been speculated that they shared the aspiration of many of their submariner colleagues of accumulating sufficient savings to afford an apartment in St. Petersburg, or at least enough to retire to southern Russia where the weather was more tolerable. However, given their sporadic and low pay (even as officers) and the fact

48 M. Kulik, 'Exclusive: Some Problems of Storing Nuclear Materials in the Northern Fleet (Russian)' (1995) in Yadernyy Control No.2.
49 Rensselaer Lee, Smuggling Armageddon (1999). New York: Saint Martin's Press.
50 M. Kulik, 'Exclusive: Some Problems of Storing Nuclear Materials in the Northern Fleet (Russian)' (1995) in Yadernyy Control No.2.
51 NTI, 'One Point Safe' (1997). Available online at: http://www.nti.org/analysis/articles/one-point-safe/ [last accessed 14.09.2018].

that Oleg had already retired, without drastic action this was likely an unattainable dream. Fluctuating exchange rates, soaring inflation and declining wages had left each individual earning approximately $1,000 per annum (often paid in arrears). Dmitriy later expressed that they had hoped to sell the stolen uranium for $300,000-500,000, which even after being split three ways, would have 'solved all their [financial] problems at once'.[52]

Their sense of economic hopelessness was further compounded by their loss of societal privileges accrued during the Soviet period. Working as a serviceman no longer carried the same prestige and perks, and following the Chernobyl disaster, nuclear work was viewed with a special negativity. As the Norwegian NGO (non-governmental organisation) Bellona states: 'The Russian naval officer [...] [had] fallen from being one of the most privileged members of Soviet society to one whose work is far less valued'.[53] The contraction of Defense spending in post-Soviet Russia also meant that the likelihood for future promotion prospects was diminishing, further motivating the perpetrators to seek alternative methods to augment their income.[54]

Preventative Measures and Security Systems

During Soviet times, insider threat prevention programmes consisted largely of political commissars, coupled with vetting for loyalty to the Communist Party. However, these had been disbanded following the end of the Cold War.[55] While the FSK (Federal Counterintelligence Service), formerly the KGB and later the FSB, were nominally responsible for human reliability and background checks, the pervasive intelligence apparatus employed by the Soviet state was in the process of being dismantled. Prior to this, the Soviet state security apparatus and restrictions on liberties had limited the opportunities for insider actions, organised crime and terrorism.[56] The combination of a clear political purpose, social security, little opportunity to profit from malfeasance, geographic isolation and the likelihood of heavy coercive punishment contributed to the minimisation of an insider threat amongst soviet submariners. However, the end of the Cold War marked a reversal for these conditions. Coercive factors ensuring reliability weakened, societal and economic perks disappeared, and corruption increased.[57] It is therefore unsurprising that those who had previously been deemed reliable were now willing to act against their employers in the hope of securing their own economic welfare.

Given the challenges in ensuring human reliability at the Sevmorput shipyard, greater emphasis should have been placed on physical security designed to protect the nuclear material on site. However, as was the case with preventative human reliability programmes, the overall security regime in place during the Soviet era had largely been reliant on the pervasive state security systems deterring insider actions in the first place, and as such, extensive on-site physical security was not prioritised.[58]

Sevmorput was one of the largest naval shipyards in Russia and had been active since 1938, servicing nuclear powered vessels since the 1960s. While it had once employed 5500 workers, by late 1993 the yard was in a state of disrepair due to a lack of work, and resources were spread thin over the sprawling site.[59] When the poor economic conditions in post-Soviet Russia routinely led to the navy receiving less than half its listed budget, it was predictable that physical

52 V. Litovkin, 'In the Northern Fleet - nuclear alarm (Russian)' (1994) in Vecherniy Murmansk, p.6.
53 Thomas Nilsen, Igor Kudrik & Alexandr Nikitin, 'Chapter 1: The Northern Fleet - The Russian Northern Fleet' (1997) in SPB.Org.Ru. Available online at: http://spb.org.ru/bellona/ehome/russia/nfl/nfl1.htm [last accessed 14.09.2018].
54 Ibid.; Bukharin & Potter, 'Potatoes were guarded better' (1995) in Bulletin of the Atomic Scientists, 51/3, p. 46.
55 Oleg Bukharin, 'Upgrading Security At Nuclear Power Plants In The Newly Independent States' (1997) in The Nonproliferation Review, 4/2, pp. 28-39.
56 Bukharin & Potter, 'Potatoes were guarded better' (1995) in Bulletin of the Atomic Scientists, 51/3, p. 46; Wendy, L. Mirsky, 'The Link Between Russian Organized Crime And Nuclear-Weapons Proliferation: Fighting Crime And Ensuring International Security' (1996) in University Of Pennsylvania Journal Of International Law, 16/4, pp. 749-781.
57 Bukharin & Potter, 'Potatoes were guarded better' (1995) in Bulletin of the Atomic Scientists, 51/3.
58 Olge Bukharin, 'Upgrading Security At Nuclear Power Plants In The Newly Independent States' (1997) in The Nonproliferation Review, 4/2, p. 33.
59 Thomas Nilsen, Igor Kudrik & Alexandr Nikitin, 'Chapter 1: The Northern Fleet - The Russian Northern Fleet' (1997) in SPB.Org.Ru. Available online at: http://spb.org.ru/bellona/ehome/russia/nfl/nfl1.htm [last accessed 14.09.2018].

protective systems were also undergoing a process of decay. A further factor undermining the implementation of security measures at the Sevmorput shipyard was that the facility was a military base. It was therefore not overseen by the Gosatomnadzor nuclear 'watchdog', a new institution tasked with improving nuclear security. Instead, the site's maintenance and protection were left under the purview of the Ministry of Defence. Given their severe budget constraints and the primacy of maintaining military capability, they predictably did not prioritise spending on preserving security and only provided limited 'regulatory' oversight.[60]

Incident Summary

According to Russian Court documents, Aleksei, Dmitriy and Oleg started to discuss stealing and subsequently selling nuclear fuel to secure their retirement between July and August 1993.[61] Most sources credit Oleg with being the 'mastermind' behind the heist, but it was clear that Dmitriy knew the most relevant technical and security information. Serious planning appears to have started from August 1993 with Dmitriy Tikhomirov briefing his brother on how to dismantle the fuel elements to maximise the amount of uranium obtained and how to do it safely. Nevertheless, the main consideration that prolonged how long they planned for was how to conduct the heist without violence. While details on their planning process are lacking, it appears that they wanted to conduct the theft non-violently and would therefore have likely spent time reviewing the functional state of the protective systems on site.

Unfortunately, Michael Kulik would later uncover that 'potatoes were guarded better' than the uranium fuel elements stored at Sevmorput.[62] On a superficial level, the physical security measures in place were reasonable, but nearly all protective security systems were in a poor state of repair or badly implemented. For instance, the base was ringed by a dual layer of wire mesh fencing, separating the perimeter, outer and inner secure areas. However, the fences were dilapidated, with multiple holes in them. Attempts had been made to patch them up with planks of wood, but these had quickly rotted and would have proven no substantial barrier. Additionally, the roads to the base and entrance gates were unguarded and there was no cleared perimeter, so the base could be approached with impunity. There was also no protection on the side of the base facing the sea. Kulik remarked than anybody wanting access to the base could have simply landed unchecked within the secure area in a rowing boat.[63]

While there were numerous safety systems monitoring the fuel storage bunker, the installed security systems were below standard. Firstly, the door to the fuel storage building was insecure. While it was a specified security requirement that the lock be embedded in the door to make cutting it harder, this regulation had been ignored and a simple padlock secured the nuclear fuel storage building. There was also a simple alarm system connected to the door that would signal if somebody entered the building. It was designed to send an alarm to the nearest guard booth if triggered (which was reportedly around 100m away from the fuel bunker and out of visual range). While it was later found that the wires and switchboards connecting the alarm to the booth were exposed and could be disconnected without consequence, it appears that this would have been unnecessary. Instead, the connections wiring the alarm system had become corroded over time, had never been repaired and had failed to function.[64] Therefore, no effort was required by Aleksei to defeat this system as he entered the building.

60 NTI, 'Nuclear Security and Gosatomnadzor' (1996). Available online at: http://www.nti.org/analysis/ articles/nuclear-security-and-gosatomnadzor/ [last accessed 14.09.2018].
61 M. Kulik, 'Exclusive: Some Problems of Storing Nuclear Materials in the Northern Fleet (Russian)' (1995) in Yadernyy Control No.2.
62 Ibid.
63 Ibid.
64 Bukharin & Potter, 'Potatoes were guarded better' (1995) in Bulletin of the Atomic Scientists, 51/3.

The guards themselves were also supposed to provide an additional layer of security. However, the actual number of guards stationed at the Sevmorput naval base was below their required compliment.[65] This situation was further exacerbated at night where only two elderly guards were stationed in proximity to the fuel storage area. While they were armed with pistols, they reportedly lacked weapons training. Even discounting the understaffing, the task of detecting intruders was made harder by conditions within the base. At night, there was no flood lighting, and refuse metal and other industrial detritus was scattered throughout the base, blocking lines of sight. The guards on the base reportedly patrolled infrequently due to the harsh weather conditions, preferring instead to remain in their guard houses for shelter.

With apparent knowledge of these limitations, Oleg, Aleksei and Dmitriy reportedly decided to proceed with their plot. On 27th November 1993, around midnight, Aleksei and Oleg drove to Sevmorput. After being dropped off near the base by Oleg, court documents note that Aleksei slipped through an unprotected gate equipped with only wire cutters, a hacksaw, a torch and a replacement padlock. Aleksei climbed through a hole in the inner fence near to fuel storage area, which his brother had briefed him on. With the use of his hacksaw, Aleksei cut through the padlock on the back door of fuel storage building in a matter of minutes, then pried open the heavy door with a discarded metal pole he found on the ground. Aleksei moved into the building, uncovered the fuel elements, and proceeded to break off three of the components he had been told contained enriched uranium, which he then placed into a bag. While the plan had proceeded flawlessly up to this point, Aleksei's rushed exit from the scene would prove to be his undoing. In his haste, he failed to shut the door properly, replace the lock or remove his pry bar or the remains of the original padlock. Nevertheless, Aleksei retraced his path out of the base and was picked up by Oleg within two hours of the initial break-in. Oleg and Aleksei drove back to Oleg's house in Polyarny, where they stored the fuel assemblies in Oleg's garage. The stolen elements contained 4.5 kilograms of uranium, of which one kilogram was uranium 235.

Although the theft had not been detected while underway, a guard patrol the next day realised that the door to the fuel storage bunker was ajar. Upon further inspection, the remains of the lock and the pry bar were found and it was quickly noticed that fuel had been stolen. It has been speculated that the theft may have remained undetected for a decade had no evidence of the theft been externally visible. Fuel elements were only individually inspected upon arrival and on being sent for reprocessing. Nevertheless, Aleksei's apparent mistake quickly raised the alarm, making this incident one of the few nuclear material thefts in the former Soviet Union detected rapidly on-site.[66] Despite this, there were few leads for the authorities to act upon and they had no clear suspects in mind.

> **"IT HAS BEEN SPECULATED THAT THE THEFT MAY HAVE REMAINED UNDETECTED FOR A DECADE HAD NO EVIDENCE OF THE THEFT BEEN EXTERNALLY VISIBLE"**

While the natural instinct of the post-Soviet authorities may have been to keep the incident secret to minimise embarrassment and 'avoid panic,' the theft was widely reported on the Kola Peninsula to ensure that custom agents and border guards were on heightened alert in the hope of recovering the fuel elements. According to media reports, the military authorities promised a substantial monetary reward for the return of the fuel rods.[67] In addition, the full panoply of criminal and intelligence investigative bodies were mobilised for the recovery of the fuel. The Ministry of Internal Affairs, Military counter intelligence, FSK, the military prosecutor's staff, federal and regional police reportedly collectively devoted six hundred staff to recovering the fuel.[68] The investigation intensively focused on major transit areas such as ports, airports and rail junctions. Major cities like Moscow and St. Petersburg had their known organised crime contacts interrogated for relevant information. While a potentially viable search strategy to counter more 'professional' nuclear smuggling, the perpetrators had not moved the fuel from the garage and therefore remained undetected. As there was no available evidence linking any of the perpetrators to the crime, Dmitriy, Aleksei and Oleg were under no special suspicion. The poor physical security conditions at Sevmorput were well known

65 V. Litovkin, 'The Criminal Trial of Three Officers of the Northern Fleet (Russian)' (1995) in Severomorsk News, 15th July 1995, p. 6.
66 Friedrich Steinhäusler & Zaitseva Lyudmila, Illicit Trafficking in Nuclear And Other Radioactive Materials As Part Of International Conference On Trafficking (2004). Courmayeur: Milan. Weltkopie, on behalf of Centro Nazionale di Prevenzione e Difesa Sociale. Available online at: http://ispac.cnpds.org/download.php?fld=pub_files&f=16.traffickingnetworksandlogisticsoftransnationalcrimeandinternationalterrorism2004.pdf [last accessed 14.09.2018].
67 V. Litovkin, 'In the Northern Fleet - nuclear alarm (Russian)' (1994) in Vecherniy Murmansk.
68 Ibid.

> **BECAUSE OF THE THEFT AND PERHAPS DUE TO THE INADEQUACIES OF THE SITE AND CAPITAL LIMITATIONS, ALL FUEL ASSEMBLIES WERE ULTIMATELY TRANSFERRED OUT OF SEVMORPUT BY 1995**

and many other employees had knowledge of where the nuclear material was stored. 500 people from Sevmorput were interviewed and 72kg of stolen mercury from the facility was recovered but no new information on the November 1993 incident was revealed. Due to a lack of leads and after several months of unsuccessful investigation, the search was scaled back.[69]

However, the military prosecutor's office persisted with the case and realised that the theft must have been carried out by an insider with intimate knowledge of the fuel elements. In addition to the potential familiarity with the lack of security on site, only safe fresh fuel had been targeted rather than irradiated fuel that had been in a reactor which would have been unsafe to handle. When Aleksei reportedly broke up the fuel elements after being briefed by Dmitriy, he had only removed the sections containing enriched uranium. This meant that the perpetrator had either been instructed or already possessed good working knowledge of the fuel elements stored on site. This led to those on site with such knowledge, including Dmitriy, to be placed under increased surveillance.

While the investigation was beginning to narrow down on Dmitriy and his associates after the seven months in which they had remained undiscovered, his hubris would finally lead to their collective downfall. On the night of 29th June 1994, Dmitriy was reportedly drinking with friends and drunkenly boasted that he had a kilo of uranium fuel for sale. Dmitriy asked a fellow officer, Lieutenant Parolov, for help in finding a contact to complete the sale of the material obtained from the theft. Parolov quickly reported this exchange to his superiors, and Dmitriy was promptly called in for questioning the next day. Finding Dmitriy talkative, Alexei and Oleg's complicity was rapidly revealed and the uranium was promptly recovered from Oleg's garage. After the conclusion to their trial in 1995, Alexei and Oleg were found guilty and sentenced to three and a half years in prison. According to Russian court documents, Dmitriy only received a suspended sentence, despite his role in coaching Alexei in how to conduct the theft, as he had not physically participated in the heist.[70] Whether these sanctions contributed to preventing insider threats within the Russian Northern fleet is debatable given their lenient nature.

In the aftermath of the incident, remedial action was taken to improve the physical security of the site to act as a deterrent against further theft of nuclear material. However, these changes were modest in scope and scale. More guards were stationed on site and were issued with portable radios, holes in the perimeter fence were boarded up, and barbed wire was added. The fuel elements in the bunker were checked routinely after the heist, but there were questions over the frequency and thoroughness of these searches. More elaborate and expensive security systems such as an additional volumetric alarm for the fuel bunker and installing CCTV were proposed but were never apportioned funding. Kulik highlighted that even some modest physical security upgrades that were suggested, such as better guard station placement, were never implemented. Because of the theft and perhaps due to the inadequacies of the site and capital limitations, all fuel assemblies were ultimately transferred out of Sevmorput by 1995.[71] It appears that little was done to improve preventative measures against insider threats following this incident, and correspondingly, similar events continued throughout the '90s in post-Soviet Russia.

69 Ibid.
70 M. Kulik, 'Exclusive: Some Problems of Storing Nuclear Materials in the Northern Fleet (Russian)' (1995) in Yadernyy Control No.2.
71 Thomas Nilsen, Igor Kudrik & Alexandr Nikitin, 'The Russian Northern Fleet Naval yards' (1997) in SPB.Org.Ru. Available online at: http://spb.org.ru/bellona/ehome/russia/nfl/nfl5.htm [last accessed 14.09.2018].

Case Study 5: Incident at Gadzhiyevo Naval Base Incident, Russia

Perpetrator Profiles

In contrast to the previous case, the incident at the Gadzhiyevo Naval Base in September 1998 involves a violent insider named Alexander Kuzminykh, a 19-year-old from St. Petersburg. After failing to get into either medical or technical school, Alexander was conscripted and subsequently volunteered to serve his term in the submarine service.[72] He reportedly passed both his initial and more thorough submariner medical and psychological examinations with high marks. Both tests had failed to uncover or report that Alexander Kuzminykh had a history of mental health issues since childhood, a habit of 'inhaling intoxicants' and enjoyed graphically violent films and books.[73] Due to his mental health issues, Alexander had been deemed ineligible for military service, but this was apparently overlooked by the St. Petersburg recruitment office.[74] Nevertheless, Alexander served most of his term unremarkably on the Akula-II class attack submarine "Vepr" and was two-thirds of the way through his conscription. His colleagues would later describe him as a sullen, withdrawn character with a fragile ego who earned the nickname 'Gloomy'.[75]

The submarine Vepr was one of the most modern vessels in service in the Russian navy and was kept at a high state of readiness. This heightened alert meant the crew was kept close to the vessel with reduced leave. Some accounts believe that this heightened alert would have limited bullying due to increased command oversight but this is disputed.[76] Other accounts report that conscripted sailors, including Alexander, were forced in line with the prevailing hierarchical culture to handover money, rations and clothes over to more senior servicemen, as well as being made to do jobs senior sailors preferred not to do themselves.[77] Others still report that Alexander was repeatedly berated by his colleagues for being slow and stupid.[78] While only recognised in retrospect, this would have been an especially unhealthy environment for Alexander. Naturally reclusive, Alexander internalised his resentment. He was unable to leave this hostile environment and appears to have built up a grudge over time.

72 Elizaveta Maetnaya & Sergey Prokopenko, 'Before Death, Sailor Kuzminykh Asked For Music To Be Put On (Russian)' (1998) in Viperson.Ru. Available online at: http://viperson.ru/uploads/attachment/file/ 351513/kp89f004.txt [last accessed 14.09.2018].

73 V. Gudkov, 'Turn on the music and get ready for death (Russian)' (June 1999) in Kommersant. Available online at: https://www.kommersant.ru/doc/219627 [last accessed 14.09.2018]; Simon Saradzhyan, 'Sailor Kills Himself After Standoff In Sub' (1998) in The Moscow Times. Available online at: http://old.themoscowtimes.com/ news/article/sailor-kills-himself-after-standoff-in-sub/285080.html [last accessed 14.09.2018].

74 Alexandra Dorfman, 'The "Boar's" Last Campaign. Sailor Kuzminyh Held The Country Hostage (Russian)' (2017) in Kazan.Aif.Ru. Available online at: http://www.kazan.aif.ru/society/posledniy_pohod_veprya_kak _matros_kuzminyh_derzhal_v_zalozhnikah_stranu [last accessed 14.09.2018].

75 Ibid.

76 V. Gudkov, 'Turn on the music and get ready for death (Russian)' (June 1999) in Kommersant. Available online at: https://www.kommersant.ru/doc/219627 [last accessed 14.09.2018].

77 Khmelnov & Chukhraev, The Rioting Fleet of Russia: From Catherine II to Brezhnev (Russian) (2015), Chapter 1.4. Available online at: www.amzn.com/B0716D9LXR [last accessed 14.09.2018].

78 Moskovsky Komsomolets, 'Sailor Shot 8 People during His Breakdown (Russian)' (1999) in Mk.Ru. Available online at: https://www.mk.ru/editions/daily/article/1999/05/20/139657-matros-rasstrelyal-8-chelovek-za-to-chto-ego-obzyivali-tormozom.html [last accessed 14.09.2018].

Incident Summary

What finally triggered Alexander into action around midnight on 10/11th September 1998 is unclear. Early media reports claim that Alexander had been temporarily confined for a disciplinary infraction, but this is not repeated in later and more detailed accounts.[79] Nevertheless, in the early morning of the 11th, Alexander ambushed the only armed watchman on duty with a chisel, wounding him severely with a blow to the head. While there were supposed to be two armed watchmen at any given point, this requirement had been dropped in the face of manpower shortages. While attempting to recover the watchman's rifle, Alexander was interrupted by a junior officer on routine patrol. Seeing the wounded sailor, 3rd class captain Besedin rushed to his aid but was also struck on the head with the chisel by Alexander. Recovering quickly, Besedin and Alexander struggled briefly, but Alexander recovered the gun and shot into the darkness, presuming he had killed Besedin. Alexander then killed the watchman with the rifle and proceeded to descend into Vepr. Still alive, Besedin raised the alarm both to the adjacent submarine and warned Vepr's bridge crew that an armed assailant was active. While they should have immediately locked the bulkheads, they responded too slowly.

Now inside the submarine and armed, Alexander passed through an occupied compartment and shot an additional five sailors dead. Proceeding into the torpedo area, Alexander activated the fire suppression system to flood the rest of the ship (having isolated his room first) with toxic haloalkane gas. This triggered the fire alarm and distracted the rest of the crew aboard who were forced to evacuate. Alexander found two additional sailors in the torpedo compartment, both of whom were conscripts with whom he had trained with. One of them, Alexei, was one of Alexander's few friends, but Alexander killed both regardless.[80] Alexander then locked the main bulkhead door to the torpedo compartment, effectively isolating himself. The only other entrance to the compartment was a narrow torpedo loading hatch which he had control over.[81]

This set the stage for a subsequent twenty-hour long standoff. While Besedin's alarm had put the base on alert, there was little that could be done to dislodge Alexander. The reactor on the Vepr was shut down and the fleet went on general alert. The submarine was surrounded and an FSB (Federal Security Service of the Russian Federation) anti-terrorist commando team that had been training in the area was scrambled to the site. Having isolated the torpedo compartment, Alexander could also not be gassed out of his position as happened in the subsequent 2002 Moscow theatre incident. Alexander threatened to detonate the torpedoes in the event of an assault, and any breaching explosive on the bulkhead door could have resulted in a detonation regardless.[82] As a precaution in the event of the torpedoes exploding, all nearby naval vessels were moved away from the Vepr.

Throughout the day, multiple failed attempts were made by senior fleet officers, a priest, a psychologist and eventually Alexander's mother and older brother (who were flown in from St. Petersburg) to convince Alexander to surrender peacefully. Alexander made no demands other than food, cigarettes, wine and a phone. Although he once asked for a helicopter, he quickly abandoned the idea of escape. Even at this stage, Alexander's behaviours appeared unhinged. From 11:00am on 11th September, Alexander communicated with the negotiators that he was going to sleep and was not heard from for four hours. At 6:25pm, Alexander stated that he was getting bored and demanded that music be played through the submarine's intercom. When his family failed to get him to surrender and Alexander started to threaten to detonate the torpedoes again, the FSB commando team acted. The final events that resulted in Alexander's death are unclear. Early reports claim that he was shot by the FSB team during an assault. Other sources claim that Alexander shot himself when the FSB

79 Associated Press, 'Russian Sailor Kills 8 On Submarine' (1998). Available online at: http://nl.newsbank. com/nl-search/we/Archives?p_multi=DNJ&p_product=PHNP&p_theme=phnp&p_action=search&p_maxdocs=200&s_trackval=PHNP&s_dispstring=Russian%20sailor%20kills%208%20on%20submarine%20AND%20date(all)&p_field_advanced-0=&p_text_advanced-0=(Russian%20sailor%20kills%208%20on%20submarine) [last accessed 14.09.2018].

80 Khmelnov & Chukhraev, The Rioting Fleet of Russia: From Catherine II to Brezhnev (Russian) (2015), Chapter 1.4. Available online at: www.amzn.com/B0716D9LXR [last accessed 14.09.2018].

81 V. Gudkov, 'Turn on the music and get ready for death (Russian)' (June 1999) in Kommersant. Available online at: https://www.kommersant.ru/doc/219627 [last accessed 14.09.2018].

82 Ibid.

team was preparing to storm down the torpedo loading hatch. More recent sources claim that the phone that Alexander used to talk with the negotiators with was rigged with a small explosive charge that killed him. On inspection of the torpedo compartment, it was observed that Alexander had piled all flammable material under the torpedo fuelling station.[83]

Had the torpedoes been detonated, there is some dispute as to what damage would have resulted. On the one hand, Norwegian authorities were reportedly braced for major radiation incident and a regional FSB director retrospectively warned of 'another Chernobyl' had there been an explosion.[84] On the other, more sceptical evaluations highlighted the difficulty of detonating the torpedoes with only fire (given the stability of the explosives). Had there been an explosion, such as with the Kursk submarine in 2000, Russian nuclear submarine design protected the reactor from damage and a breach may not have occurred.[85] There were also no nuclear weapons aboard the Vepr at the time of the incident. The reactions of the authorities in moving nearby submarines away from the area suggests that there was a credible threat to all nearby facilities and vessels in the immediate area.

In the aftermath of the incident, the reform most quickly implemented was enforcement of the requirement for two armed watchmen to be on duty at any given time.[86] In addition, many senior officers involved in the incident, including the commander of the Northern Fleet itself, received demotions and reprimands.[87] However, the most important reforms to prevent similar incidents were those that raised the standards for personnel employed on Russian nuclear submarines. Not only were conscripts barred from serving on nuclear submarines following this incident, but the requirements for selection and frequency of psychological testing were increased.[88]

83 Ibid.

84 AFIO Intelligence Notes, 'Issue 36 - 22 September 1998' (2018). Available online at: https://www.afio.com/ sections/wins/1998/notes36.html [last accessed 14.09.2018]; Igor Kudrik, 'Shoot-Out On Nuclear-Powered Submarine' (1998). Available online at: http://bellona.org/news/nuclear-issues/accidents-and-incidents/1998-09-shoot-out-on-nuclear-powered-submarine [last accessed 14.09.2018].

85 Submarines.narod.ru, 'Post Clearance: Accidents and Incidents (Russian)' (2002). Available online at: http://www.submarines.narod.ru/s_p.html [last accessed 14.09.2018].

86 Gudkov, V., 'Turn on the music and get ready for death (Russian)' (June 1999) in Kommersant. Available online at: https://www.kommersant.ru/doc/219627 [last accessed 14.09.2018].

87 Ibid.

88 Simon Saradzhyan, 'Dynamics of Maritime Terrorist Threats to Russia and the Government's Response' (2009) in Connections: The Quarterly Journal, 8/3, pp. 65-66.

Recap and Broader Issues

Both these cases illustrate several systemic issues in Russia in the 1990s that contributed to an increased frequency of insider threats. Namely, sustained economic turbulence, budgets at breaking point for the Russian navy, and a considerable inventory of nuclear materials protected by degraded security systems. In addition, shortages of manpower plagued the armed services, meaning that standards for those conscripted into military service were falling. Once in service, conditions such as a lack of leave, pay in arrears, extreme bullying, drug abuse and even food shortages meant that violent insider incidents were not infrequent.[89] For example, the NGO Bellona reported in September 1998 that servicemen in the Northern fleet had not been paid since May that year.[90]

> It is worth re-emphasising that these two insider incidents were not isolated cases. Thefts of nuclear material in the Northern Fleet were not uncommon in the 1990s. Another attempted insider theft of uranium had already occurred in July 1993 and four more alleged cases of nuclear materials theft were reported between 1994 and 1999.[91] Only several days before Alexander's rampage, five sailors from Dagestan, who wanted to return to the Caucasus, mutinied at another nuclear facility on Novaya Zemlya. They killed a guard and took forty-eight hostages before they were killed in turn by the authorities. In another violent incident that occurred in 1999 at the Gremikha naval base, two guards killed three of their colleagues and wounded several others. While no definitive motive was established, drugs and/or bullying were blamed.[92]
>
> As seen in both examined cases, physical security was weak and provided little deterrent, conditions for servicemen were poor, and institutions lacked the capacity or willingness to sort potential insiders out of their diminished manpower pools. It is therefore unsurprising that the economic recovery in Russia through the 2000s improved conditions within the armed services, seemingly reducing the frequency and severity of insider incidences. Similarly, as state institutions with a purview over intelligence and justice functions started to recover and reform after the collapse of the Soviet Union, they contributed to the more thorough screening of potential insiders and the tackling of organised crime.[93] While bullying remains a problem in the Russian armed services, reforms such as lowering the reliance on conscripted manpower through the reduction of the conscription period to one year have also

89 Anatoly Safonov, 'Hazing In the Andreeva Bay (Russian)' (2009) in Andreeva.1Gb.Ru. Available online at: http://andreeva.1gb.ru/story/dedovshina.html [last accessed 14.09.2018].

90 Igor Kudrik, 'Shoot-Out on Nuclear-Powered Submarine' (1998). Available online at: http://bellona.org/news/ nuclear-issues/accidents-and-incidents/1998-09-shoot-out-on-nuclear-powered-submarine [last accessed 14.09.2018].

91 Moltz & Robinson, 'Dismantling Russia's Nuclear Subs: New Challenges to Non-Proliferation' (1999). Available online at: www.armscontrol.org/act/1999_06/subjun99 [last accessed 14.09.2018].

92 I. Zhevelyuk, 'Distributed In the Island (Russian)' (2000). Available online at: http://gremih.ru/publikacii/49-rastrel.html [last accessed 14.09.2018].

93 Simon Saradzhyan, 'Dynamics of Maritime Terrorist Threats to Russia and the Government's Response' (2009) in Connections: The Quarterly Journal, 8/3, pp. 53-84.

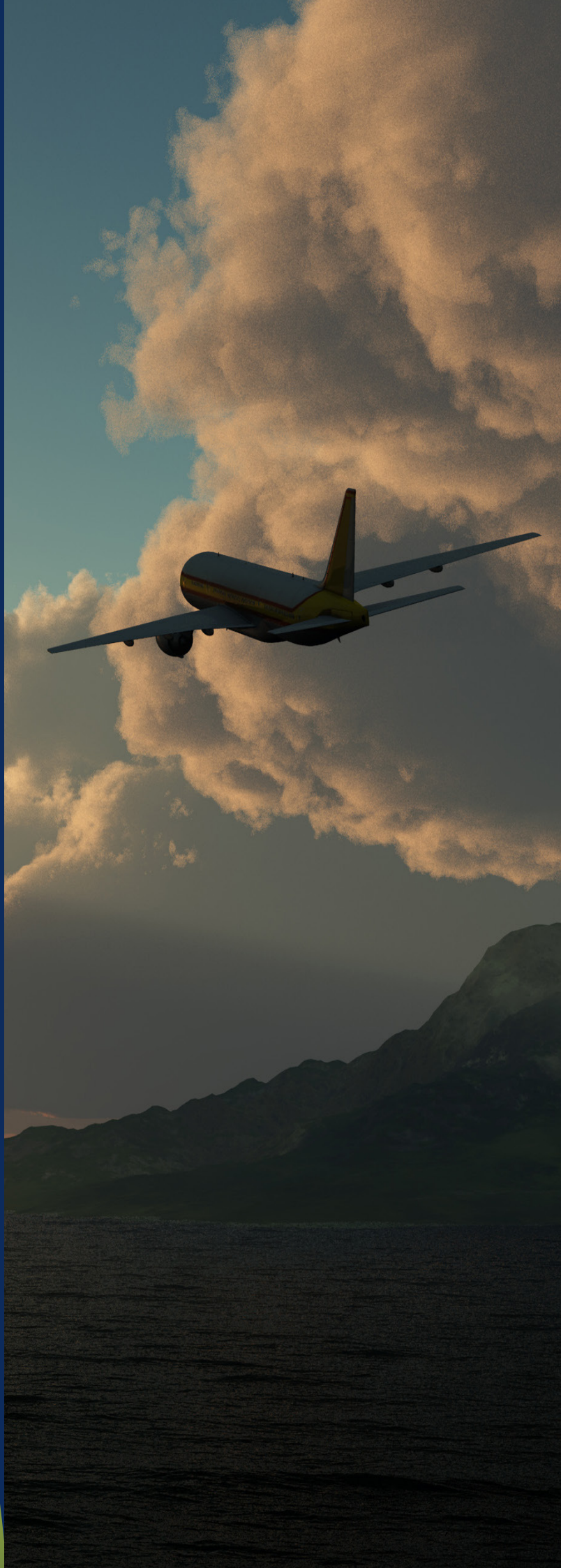
helped. In regard to the security of nuclear material, while the decommissioning of former Soviet submarines has been far from ideal and required considerable foreign assistance, it has consolidated vessels awaiting decommissioning into fewer sites and increased serviceability and professionalism in the remaining Russian nuclear submarine fleet.[94]

Suggested Discussion Points:

- How can poor national economic circumstances be prevented from challenging worker satisfaction?
- What role do protective measures have in preventing insider threat actions (do they serve as a deterrent)?
- Do bullying and poor worker conditions lead to violence and radicalisation? What systems can be put in place to prevent this?
- If a nuclear site is due to be decommissioned and jobs lost, do the employees pose an increased security risk?

94 Paul Marks, 'How Do You Dismantle a Nuclear Submarine?' (2015). Available online at: http://www.bbc.com/future/story/20150330-where-nuclear-subs-go-to-die [last accessed 14.09.2018]; Moltz & Robinson, 'Dismantling Russia's Nuclear Subs: New Challenges to Non-Proliferation' (1999). Available online at: www.armscontrol.org/act/1999_06/subjun99 [last accessed 14.09.2018].

Insider Threats in the Aviation Industry and Other Critical Infrastructure



Introduction

This section presents three case studies from the aviation industry, considering efforts to address insider threats using preventative measures at airports, and in the cockpit environment. The first case considers how airport workers can constitute an insider threat and focuses on the preventative measures taken at airports in the United States to mitigate these risks. The second and third cases consider specific insider incidents involving airline pilots, starting with the case of Germanwings flight 9525 in which pilot Andreas Lubitz crashed a plane of 200 passengers into a mountain in an apparent murder-suicide in 2015. The third case considers the suicide bombing of Daallo Airlines flight 159 after its departure from Mogadishu in 2016.

IN 2014

1.2 MILLION PEOPLE WERE EMPLOYED IN THE 485 AIRPORTS IN THE U.S.

A significant number of individuals work at airports in a wide variety of roles, from implementing airport security, to conducting maintenance on and dispatching aircraft, to staffing shops, bars and restaurants. Many airport employees have access to secure areas of the airport, such as aircraft stands, maintenance areas, cargo loading facilities and airside passenger amenities. There have been several cases where airport employees have been involved in perpetrating, or co-opted into, committing acts of terrorism. Airport workers have also been radicalised and travelled overseas to join terrorist groups. Furthermore, employees have used their insider status to facilitate other types of criminal activity, such as smuggling contraband such as narcotics and arms on commercial flights. Airline pilots also typically have similar access, with of course additional particularly sensitive cockpit access while the plane is in flight.

Significant measures, both protective and preventative, have been put in place to mitigate insider security risks at airports. However, implementing these measures within large occupational groups has proved challenging. For example, in 2014 the 485 airports in the U.S. employed over 1.2 million people, and in 2015 it was estimated that there were 130,000 licensed commercial pilots around the world. It is clear that preventative measures have been implemented unevenly across the globe, and even within specific countries. Consequently, despite these measures, security and criminal incidents at airports and involving commercial flights continue to be perpetrated by insiders.

Case Study 6: Airport Security and Preventative Measures in the United States

The U.S. Transport Security Administration (TSA) and Federal Bureau of Investigation (FBI) have noted that the insider threat posed by 'rogue aviation workers' to be 'pressing'.[95] A 2017 report of a U.S. Congressional Committee also noted 'increasing concerns that insider threats to aviation security are on the rise'.[96] While the scale of the issue is unclear, some statistics do provide insight. Between 2003 and 2015, the TSA directed airports to deny or revoke a total of 58 airport badges allowing access to secure areas for applicants and existing badge holders following vetting procedures.[97] A 2015 U.S. Department for Homeland Security (DHS) report suggested that 73 aviation workers with links to terrorism were currently or had recently been employed at U.S. airports with access to secure areas.[98] These were missed by TSA vetting, although further investigation suggested they did not pose a threat.[99]

Due to the diversity in national approaches, and the availability of information in the U.S. context, this case study takes a U.S.-focus by considering preventative measures at U.S. airports. The case study provides context to the insider threat in the aviation industry, outlines preventative measures taken at airports, and considers some challenges to implementing preventative measures.

The Aviation Industry and Insider Threats

The aviation and airport industries have a huge number of employees – 1.2 million in the U.S. alone.[100] The busiest airport in the world, Atlanta Hartsfield Jackson, employs 63,000 people and is the largest employer in the state of Georgia. Many airport employees have access to secure or 'sterile' areas of the airport, such as aircraft stands, maintenance areas, cargo loading facilities and airside amenities for passengers. Airports also frequently employ large numbers of contractors. For example, in the U.S. over 50,000 construction workers are employed at airports annually, also potentially with access to secure areas.[101]

95 Jennifer A. Grover, 'Aviation Security: Airport Perimeter and Access Control Security Would Benefit from Risk Assessment and Strategy Updates' (May 2016) in Government Accountability Office report, GAO-16-632. Available online at: https://www.gao.gov/assets/680/677586.pdf [last accessed 17.09.2018].
96 Homeland Security Committee, 'America's Airports: The Threat from Within' (February 2017) in House of Representatives Homeland Security Committee Majority Staff Report. Available online at: https://homeland. house.gov/wp-content/uploads/2017/02/Americas-Airports-The-Threat-From-Within.pdf [last accessed 17.09.2018].
97 Sub-Committee on Transportation Security, 'How TSA Can Improve Aviation Worker Vetting' (June 2015), Congressional Hearing, 114th Congress, 1st Session. Available online at: https://www.gpo.gov/fdsys/pkg/CHRG-114hhrg96167/html/CHRG-114hhrg96167.htm [last accessed 17.09.2018].
98 Department of Homeland Security Office of the Inspector General (DHS OIG), 'TSA Can Improve Aviation Worker Vetting (Redacted)' (June 2015), OIG-15-98. Available online at: https://www.oig.dhs.gov/assets/ Mgmt/2015/OIG_15-98_Jun15.pdf [last accessed 17.09.2018].
99 Sub-Committee on Transportation Security, 'How TSA Can Improve Aviation Worker Vetting' (June 2015), Congressional Hearing, 114th Congress, 1st Session. Available online at: https://www.gpo.gov/fdsys/pkg/CHRG-114hhrg96167/html/CHRG-114hhrg96167.htm [last accessed 17.09.2018].
100 CDM Smith, 'The Economic Impact of Commercial Airports in 2013' (September 2014), in Report prepared for the Airports Council International – North America. Available online at: https://www.aci-na.org/sites/default/ files/economic_impact_of_commercial_aviation-2013_update_final_v10.pdf [last accessed 17.09.2018].
101 Ibid.

AS OF 2017

ONLY THREE U.S. AIRPORTS CONDUCTED 100% SECURITY SCREENING OF STAFF AND THEIR BAGS WHEN ENTERING THE SECURE AREA OF WORK

Malicious insiders at airports can use their access, knowledge and authority to commit criminal or terrorist acts. The U.S. TSA and FBI provide a broad definition of insider threats to aviation security, defining the insider threat:

> *to include threats to all aspects of aviation security, including passenger checkpoint, baggage, cargo screening, access controls, perimeter security, and off-airport aviation-related operations and activities, among other things.*[102]

There have been a handful of cases where airport employees have been involved in perpetrating, or co-opted into, committing acts of terrorism.[103] More commonly, airport employees have also used their insider status to facilitate other types of criminal activity, such as smuggling contraband such as narcotics and firearms.[104]

The U.S. and other countries around the world have made long standing efforts to enhance aviation security following a series of hijackings in the late 1960s and early 1970s. Other terrorist and criminal events such as the 9/11 attacks have also changed the face of aviation security. In 1973 the U.S. passed some of the earliest and most formative airport security legislation which put in place access controls, mandated that airports hire private security, and of most relevance for this handbook, conduct background checks on employees.[105] That said, there were relatively few changes in airport security from the 1980s until the early 2000s. Triggered by the 9/11 terrorist attacks, a range of new security related programmes and measures were put in place. These included the creation of the TSA, designation of a 'sterile' area beyond the security check-point restricted to travelling passengers, creation of the Security Identification Display Area (SIDA), and mandating that staff with SIDA access receive a background finger-print based 'criminal history' check, as well as appropriate training.[106]

In terms of physical access control and protective measures, in March 2005 random screening conducted on airport workers was supplemented by a more extensive screening programme when entering secure areas.[107] Security incidents led some airports to adopt 'beyond-compliance' measures. For example, arrests of two airline employees at Orlando International Airport in 2007 for trying to smuggle marijuana and firearms to Puerto

Rico led the airport authority to conduct 100% screening of employees. As of 2017, only three U.S. airports conducted 100% physical screening of staff and their bags when entering the secure area to work. These are Miami International Airport, Orlando International Airport, and Hartsfield Jackson Atlanta International Airport.[108] This general lack of comprehensive physical screening places significant emphasis on preventative measures in addressing insider threats.

Current background checks conducted on employees comprise a 'security threat assessment' conducted by TSA, including a check against terrorism watchlists, a criminal history check based on fingerprint records, and verification of the applicant›s authorisation to work in the U.S.[109] TSA recurrently vets accredited airport workers every time it receives

102 Jennifer A. Grover, 'Aviation Security: Airport Perimeter and Access Control Security Would Benefit from Risk Assessment and Strategy Updates' (May 2016) in Government Accountability Office report, GAO-16-632. Available online at: https://www.gao.gov/assets/680/677586.pdf [last accessed 17.09.2018].

103 See Peter J. Greco, 'Insider Threat: The Unseen Dangers Posed by Badged Airport Employees and How to Mitigate Them' (2017) in Journal of Air Law and Commerce, Vol. 82, pp.717-742; Tom Lyden, 'Insider Threat: Side-by-side with a future terrorist at MSP Airport' (November 2014) in Fox News. Available online at: http://www.fox9.com/fox-9-mn-special-archive/insider-threat-sidebyside-with-a-future-terrorist-at-msp-airport [last accessed 17.09.2018].

104 Joe Sharkey, 'Gun Smuggling on Plane Reveals Security Oversight' (December 2014) in New York Times. Available online at: https://www.nytimes.com/2014/12/30/business/gun-smuggling-on-plane-reveals-security-oversight.html [last accessed 17.09.2018]; Max Kutner, 'TSA and Airport Exmployees Allegedly Smuggled 20 Tons of Cocaine over 18 Years' (February 2017] in Newsweek. Available online at: https://www.newsweek.com/tsa-puerto-rico-airport-cocaine-smuggling-556342 [last accessed 17.09.2018].

105 Peter J. Greco, 'Insider Threat: The Unseen Dangers Posed by Badged Airport Employees and How to Mitigate Them' (2017) in Journal of Air Law and Commerce, Vol. 82, pp.717-742.

106 U.S. Congress, 49 C.F.R. § 1540 and § 1542.

107 Homeland Security Committee, 'America's Airports: The Threat from Within' (February 2017) in House of Representatives Homeland Security Committee Majority Staff Report. Available online at: https:// homeland.house.gov/wp-content/uploads/2017/02/Americas-Airports-The-Threat-From-Within.pdf [last accessed 17.09.2018].

108 Jeff Pegues, 'TSA blasted for "insider threat" security gap' (May 2016) in CBS News. Available online at: https://www.cbsnews.com/news/tsa-blasted-for-insider-threat-security-gap/ [last accessed 17.09.2018].

109 Sub-Committee on Transportation Security, 'How TSA Can Improve Aviation Worker Vetting' (June 2016), Congressional Hearing, 114th Congress, 1st Session. Available online at: https://www.gpo.gov/fdsys/pkg/CHRG-114hhrg96167/html/CHRG-114hhrg96167.htm [last accessed 17.09.2018].

an update to the terrorist watch list. These updates can occur several times a day, and the entire directory of airport employees can be rescreened within minutes.[110] Based on this vetting process, the TSA directs the airport to grant, deny or revoke passes. The vetting process also feeds information back into intelligence assessments on insider threats, with 300 individuals being added to existing watchlists in 2014 as a result of screening.[111]

Criminal background checks take place when employees are accredited, and then with re-accreditation every two years. A new FBI programme called Rap Back (Record of Arrest and Prosecution Background) has allowed for employee criminal record checks to be conducted on an ongoing, real-time basis. The system, which effectively provides '24/7 vetting of credentialed populations', has experienced some technical difficulties. However, since 2017 it has been used to vet all TSA employees, and employees of several airports and carriers.[112]

Behavioural Observation Officers have been used by the TSA to identify potentially suspicious behaviour amongst passengers through the Screening of Passengers by Observation Techniques (SPOT) programme. This programme has used red-flag lists of suspicious behaviours to identify potential threats. Around 100 indicators have been reported in the media.[113]

Selected Indicators of Suspcious Behaviour used by TSA include:

Stress factors:
- Arriving late for the flight
- Avoiding eye contact
- Exaggerated yawning
- Excessive fidgeting

Fear factors:
- Cold penetrating stare
- Constantly looking at other travellers
- Exaggerated emotions
- Exaggerated repetitive grooming gestures

Deception factors:
- Appears confused or disoriented
- Appears to be in disguise
- Does not respond to authoritative commands

Unusual items:
- Blue prints
- Global Positioning System (GPS)
- Numerous pre-paid phone cards or cell phones

Signs of deception:
- "Adam's apple" jump
- Change in voice, pitch, rate, volume, choice of words, dry mouth

110 Department of Homeland Security Office of the Inspector General (DHS OIG), 'TSA Can Improve Aviation Worker Vetting (Redacted)' (June 2015), OIG-15-98. Available online at: https://www.oig.dhs.gov/assets/ Mgmt/2015/OIG_15-98_Jun15.pdf [last accessed 17.09.2018].
111 Ibid.
112 Homeland Security Committee, 'America's Airports: The Threat from Within' (February 2017) in House of Representatives Homeland Security Committee Majority Staff Report.. Available online at: https://homeland. house.gov/wp-content/uploads/2017/02/Americas-Airports-The-Threat-From-Within.pdf [last accessed 17.09.2018].
113 Jana Winter and Cora Currier, 'Exclusive: TSA's Secret Behaviour Checklist to Spot Terrorists' (March 2015), in The Intercept. Available online at: https://theintercept.com/2015/03/27/revealed-tsas-closely-held-behavior-checklist-spot-terrorists/ [last accessed 17.09.2018].

However, the Government Accountability Office (GAO) and reporters have criticised the scientific basis for these programs.[114] These behavioural observation techniques have also been used to counter insider threats through the random screening process conducted on airport employees. 'Playbook operations' form part of random screening efforts and involve monitoring particularly busy access points where random screening of employees is carried out as the enter the secure area. TSA Behaviour Detection Officers watch for individuals displaying suspicious characteristics, especially if they appear to be seeking to avoid the random screening.[115]

Challenges in Prevention Mitigating Insider Threast to Airport Security

There are numerous challenges in mitigating the dangers posed by insider threats at airports, both through broader security measures, and specifically through preventative measures. Challenges are discussed below in three main areas: costs and disruption, collaboration between stakeholders, and data-sharing and legality.

Costs and Disruption

More broadly, implementing security measures against insiders can be costly and disruptive to operations. The clearest example of this, albeit a protective measure, is the physical screening of staff as they arrive for work and enter the secure areas. This can be timely, costly and disruptive, which is likely one of the reasons why most U.S. airports do not undertake 100% screening. Atlanta reportedly spent $5 million on equipment and hired 150 extra screening staff when it moved to 100% screening.[116] However, the fact that some of the busiest airports with the largest workforces in the U.S. (Atlanta is the busiest, Orlando and Miami are around 11th and 12th busiest) do undertake screening does show that the cost and impact on general operations is not insurmountable.

While re-screening all accredited employees every time the terrorist watchlist is reissued is largely an automated process taking just minutes, there are also manual elements. Automated screening tools often lead to 'false positives' amongst positive matches. False positives are individual's records that match or are very similar to listed names. The rescreening of near to 1 million names, sometimes several times daily generated thousands of possible matches which need manual sifting and follow-up checks annually.[117]

Collaboration Between Stakeholders

Implementing preventative measure programmes requires seamless coordination between multiple stakeholders including government, intelligence agencies, airport authorities and airlines.[118] For example, in the U.S. the airport operators collect and verify the data of those seeking credentials. The TSA oversees the vetting process itself, owning the 'screening gateway'. The FBI undertakes fingerprint checks and provides terrorist watchlist data. The data used to build the watchlist and fingerprint database are collected by a variety of U.S. law enforcement and intelligence agencies. The criminal history checks are largely conducted by the airport operators themselves using commercial services, although some are moving to use the FBI RapBack programme.

114 Stephen M. Lord, 'Aviation Security: TSA Should Limit Future Funding for Behavior Detection Activities' (November 2013) in Government Accountability Office report, GAO-14-159. Available online at: https://www.gao.gov/assets/660/658923.pdf [last accessed 17.09.2018]; Sharon Weinberger, 'Airport Security: Intent to Decieve?' (2010) in Nature Vol. 465, pp. 412-415.

115 Homeland Security Committee, 'America's Airports: The Threat from Within' (February 2017), House of Representatives Homeland Security Committee Majority Staff Report. Available online at: https://homeland. house.gov/wp-content/uploads/2017/02/Americas-Airports-The-Threat-From-Within.pdf [last accessed 17.09.2018].

116 Peter J. Greco, 'Insider Threat: The Unseen Dangers Posed by Badged Airport Employees and How to Mitigate Them' (2017) in Journal of Air Law and Commerce, Vol. 82, pp. 717-742.

117 Sub-Committee on Transportation Security, 'How TSA Can Improve Aviation Worker Vetting' (June 2015), Congressional Hearing, 114th Congress, 1st Session. Available online at: https://www.gpo.gov/fdsys/pkg/CHRG-114hhrg96167/html/CHRG-114hhrg96167.htm [last accessed 17.09.2018].

118 Department of Homeland Security Office of the Inspector General (DHS OIG), 'TSA Can Improve Aviation Worker Vetting (Redacted)' (June 2015), OIG-15-98. Available online at: https://www.oig.dhs.gov/assets/Mgmt/ 2015/OIG_15-98_Jun15.pdf [last accessed 17.09.2018].

Data Collection,Sharing and Legality

An integral element of the vetting process is the data provided by employees seeking accreditation and used to check employee applications. The challenge of ensuring the integrity and smooth running of these data pipelines relates to the challenge of collaboration and coordination between the stakeholders discussed above. Data collection undertaken by airport operators and airlines is not always collected in a standardised or optimum way. For example, 1,500 records in TSA's screening gateway included first names of two or fewer characters, with 300 of these including a single character or initial.[119] Social Security Numbers and passport numbers were not routinely collected. A 2015 audit undertaken by the DHS Inspector General noted that 'TSA needs to improve the quality of data used for vetting purposes'.[120]

TSA did not always have access to all the appropriate watchlists to screen against. For example, the 73 individuals with links to terrorism that were able to get accreditation at U.S. airports were not caught in vetting because the TSA did not have access to all terrorism-related category codes under then interagency watchlist sharing policy.[121] Bureaucratic hurdles can be challenging. It took the TSA eighteen months to secure a memorandum of understanding with the National Counterterrorism Center (NCTC) to ensure data could be shared. [122] As well as bureaucratic hurdles, legal challenges can be problematic, limiting the agencies which can undertake certain parts of the vetting process.

Suggested Discussion Points:

- Should efforts to mitigate against insider threats at airports continue to rely on preventative measures such as vetting? Or should protective measures, such as making 100% screening a requirement, be enhanced?
- Are behavioural observation programs a useful way of identifying suspicious behaviour? On what basis should indicators of such behaviour be determined?
- What are the greatest challenges to implementing a program of preventative measures? Bureaucratic, legal, technical, cultural or other?

119 Ibid.
120 Ibid.
121 Ibid.
122 Sub-Committee on Transportation Security, 'How TSA Can Improve Aviation Worker Vetting' (June 2015), Congressional Hearing, 114th Congress, 1st Session. Available online at: https://www.gpo.gov/fdsys/pkg/CHRG-114hhrg96167/html/CHRG-114hhrg96167.htm [last accessed 17.09.2018].

Case Study 7: German Wings Murder-Suicide Crash

Perpetrator Profile

Andreas Lubitz had ambitions to be a pilot from a young age and was accepted onto Lufthansa's trainee flying programme directly after graduating from high school in 2007. Lubitz, a disciplined student from a prosperous small town in south-west Germany, was among only five percent of applicants to be accepted. However, just a couple of months into the programme, Lubitz abruptly left and returned home. He was later diagnosed by a psychiatrist as suffering from a deep depressive episode involving thoughts of suicide and was treated with antidepressants and psychotherapy sessions.

According to this psychiatrist (whose name is protected by German privacy laws), Lubitz's breakdown was caused in part by the move to Bremen. Lubitz was also suffering from tinnitus – a condition that causes the sensation of hearing near-constant sound – which itself can be a symptom of depression. His family later disclosed that he had an intense fear of personal failure.

After sixth months in psychiatric care, Lubitz was certified by his doctor as fit to resume flying training. Yet in fact his treatment continued for several more months. German aviation officials accepted the doctor's recommendation but amended his trainee pilot's licence with the code 'SIC', which would oblige him to undergo regular medical examinations throughout his career to retain his licence. Lubitz would have been aware that any further mental health treatment disclosed to Lufthansa would spell the end to his pilot career.

Lubitz went on to complete his training at Bremen in 2010 and then applied for Lufthansa's flying school in Arizona. His initial application to the U.S. Federal Aviation Administration (FAA) was, however, rejected due his failure to declare his history of mental illness. Making false statements on a FAA form carries a custodial sentence under U.S. perjury laws.[123] Yet, for unknown reasons, Lubitz was allowed to resubmit his application once he had provided an up-to-date status report from his doctor. Weeks later Lubitz was in Arizona, where he amassed enough flying hours to be able to return to Germany to fly jet engine aircraft.

Lubitz then followed Lufthansa's typical career path of combining further flight training with work as a flight attendant. In September 2013, he became a fully-fledged pilot at Germanwings, a low-cost airline owned by Lufthansa. After this point, the airline did not document any further psychological episodes although it appears Lubitz took longer than the usual one-and-a-half to two years to qualify as a commercial pilot.

At Germanwings, Lubitz proceeded quickly through the ranks to first officer and was given responsibility to co-pilot short flights within Western Europe. However, his private life was beginning to unravel after his girlfriend of seven years allegedly broke off their relationship. He was also facing the possible disintegration of his eyesight, fuelling fears his flying career would end prematurely. Between late 2014 and early 2015, Lubitz began visiting a series of ophthalmologists, neurologists and psychiatrists – more than 12 in total. No diagnosis could be found for his eyesight condition, however, indicating that this may have been psychosomatic.

123 See United States of America v. James M. Culliton, 328 F.3d 1074, 9th Cir., 2003. Available online at: https://law.justia.com/cases/federal/appellate-courts/F3/328/1074/500120/ [last accessed 17.09.2018].

Lubitz appears to have deliberately taken measures to evade the suspicions of Lufthansa about his health issues during this period. In Germany there is no central database of medical files, meaning that individual doctors would not have picked up on the full extent of his health problems. He did not seek out a Lufthansa doctor and apparently failed to disclose his eyesight and psychological problems during a routine medical check-up in August 2014, which he passed.

By now, Lubitz was taking an array of powerful antidepressant medicines, whilst at least one doctor urged him to check into a psychiatric clinic. Most significantly, his doctors issued multiple notes pronouncing Lubitz unfit for work, but he failed to disclose these to Lufthansa. He also began searching the internet for ways to commit suicide and subsequently for information on the locking mechanism of a A320 cockpit door. On 24th March 2015, Andreas Lubitz deliberately crashed a scheduled passenger plane into a mountain ravine near Nice, killing all 150 people on board.

Preventative Measures and Security Systems

In 2012, the UN (United Nations) agency International Civil Aviation Organization (ICAO) criticised the airline industry for failing to provide systematic screening of pilots for signs of mental illness. The ICAO was particularly concerned about weak provisions for younger pilots, recognising that this demographic is more likely to suffer from disorders of a psychological than a physical nature. The ICAO observed that most traditional medical checks were inadequate to detect mental health issues.[124]

Despite previous documented cases of pilot suicide, however, the ICAO's 2012 recommendations to enhance psychological screening have not found traction across the aviation industry. According to the ICAO, airlines have not tended to prioritise mental health support for their workforces, often failing to recognise that appropriate provisions could potentially advert the most extreme manifestation of mental breakdown, that of murder-suicide. Indeed, the safety/security agenda has remained orientated around a triad of the technical condition of aeroplanes, the physical and cognitive aptitude of pilots, and the risk of hijacking and terrorism[125].

In 2013, European Union (EU) regulations took effect that laid out a framework for the medical assessments of airline pilots.[126] Under these binding regulations, pilots working for an airline registered in the EU are obliged to undergo medical assessments at least once a year, during which an independent aviation doctor must also assess the pilot's psychiatric and psychological status and refer any cases to the national authorities.

Germany's stringent privacy laws, however, have created tensions with these new EU regulations. In particular, information submitted by Germany's licenced aero-medical examiners tends not to be sufficiently detailed for accurate validation by the state aviation regulator (Luftfahrt-Bundesamt; LBA). Indeed, only the overall result – fit or unfit – is submitted to the LBA, with the detailed assessment itself retained by the aero-medical examiner. Moreover, psychological assessments often rely on 'self-reporting' whereby pilots fill out a questionnaire themselves.

124 ICAO, 'Manual of Civil Aviation Medicine' (May 2012), Doc 8984 AN/895. Available online at: www.icao.int/publications/Documents/8984_cons_en.pdf [last accessed 17.09.2018].

125 Ibid.

126 European Commission, 'Commission Regulation (EU) No 1178/2011 of 3 November 2011 laying down technical requirements and administrative procedures related to civil aviation aircrew pursuant to Regulation (EC) No 216/2008 of the European Parliament and of the Council' (November 2011) in Official Journal of the European Union. (N.b. took effect on 8 April 2013). Available online at: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32011R1178&from=EN [last accessed 17.09.2018].

In the case of Andreas Lubitz, Lufthansa continued to employ a standardised applicant-screening process even after the SIC code was applied to his licence. There was no monitoring or follow-up treatment beyond the assessment required for any pilot who had suffered a previous health problem. Meanwhile, the SIC coding system did not differentiate between mental and physical incapacity. Even during a press conference in the aftermath of the crash, Lufthansa's chief executive stated that Lubitz had been '100 percent' fit to fly.[127]

Back in September 2014, the EU's European Aviation Safety Agency (EASA) had urged Germany to address a number of aviation safety shortcomings, including its national laws governing the disclosure of medical records to the LBA. Nevertheless, Germany continued to resist EASA's interventions, even after the official investigation report was published which concluded that flaws in the country's medical assessment regime had contributed to the Germanwings disaster. According to European Commission officials, Germany has been the least cooperative member state in its dealings with EASA, and the agency has considered infringement proceedings against Berlin as a result.[128]

It is difficult to prove conclusively that an enhanced framework for medical assessment would have adverted the Germanwings disaster. One of the most troublesome aspects of the disaster is that Lubitz's clearance level was probably a key obstacle in him seeking out appropriate mental health treatment, knowing his future career was at stake. Nonetheless, most states with advanced aviation sectors take the more measured approach, that patient confidentiality should not be at the expense of aviation safety. In most cases, a pilot suffering psychological problems would be grounded during treatment and all medical records referred to the national authorities.

On a global level, however, there remains a conspicuous dearth of regulations or industry initiatives that actively seek to mitigate the threat of pilot suicide. Aside from privacy concerns, commercial pressures appear to be the greatest impediment, with the aviation industry facing a global shortage of trained pilots. Yet, whilst rare, pilot murder-suicide incidents have occurred and resulted in major loss of life. Moreover, such events tend to cause disproportionate numbers of deaths as compared to accidents.[129] The pilot is looking to maximise deaths, not the reverse. The U.S. Aviation Safety Network lists ten conclusive and inconclusive cases over the past 25 years (see Table 7.1).

> **"IN 2012, THE UN AGENCEY ICAO CRITICISED THE AIRLINE INDUSTRY FOR FAILING TO PROVIDE SYSTEMATIC SCREENING OF PILOTS FOR SIGNS OF MENTAL ILLNESS"**

Notably, key aviation stakeholders in many of these cases disputed the findings of the crash investigations, highlighting a widespread culture of denial around the issue of pilot murder-suicide. In the case of Royal Air Maroc flight 630, the official Moroccan investigation and a U.S. summary report both concluded that the pilot had deliberately disconnected the plane's autopilot. However, this explanation was challenged by the Moroccan Pilots' Union despite being unable to provide an alternative explanation.

In the cases of SilkAir flight 185 and EgyptAir flight 990, both the investigations were conducted by the U.S. National Transportation Safety Board (NTSB) but was rejected by their respective national authorities. In the Indonesian case, leaked reports in the media suggested that Indonesian investigators concurred with the NTSB findings but were overruled by senior management, who were concerned that the findings could make the public too frightened to fly.

These isolated pilot suicide events are so rare that it is impossible to verify patterns of behaviours in any systematic way. In their study of 65 aircraft disasters, Kenedi et al. also argue that the concepts of suicide and murder-suicide tend to be grouped together in public discourses, yet these are viewed as separate events in psychiatry with distinct risk factors.[130]

127 Siva Govindasamy & Swati Pandey, 'Suicidal Pilots hard to spot, say experts' (March 2015) in Reuters. Available online at: https://uk.reuters.com/article/uk-france-crash-airlines-psychology/suicidal-pilots-hard-to-spot-say-experts-idUKKBN0MN0ZZ20150327 [last accessed 17.09.2018].
128 J. Valero, 'Germany reluctant to strengthen pilot checks on first anniversary of Germanwings crash' (March 2016) in Euractiv. Available online at: www.euractiv.com/section/transport/news/germany-reluctant-to-strengthen-pilot-checks-on-first-anniversary-of-germanwings-crash [last accessed 17.09.2018].
129 C. Kenedi, S. H. Friedman, D. Watson & C. Preitner, 'Suicide and Murder-Suicide Involving Aircraft' (2016) in Aerospace Medicine and Human Performance, Vol. 87, No. 4, pp. 388-396.
130 Ibid.

Date	Airline or Flight Nr.	Location of Site or Flight Path	Deaths	Incident Summary
07.04.1994	Federal Express (now FedEx): Flight 705	Memphis, Tennessee, U.S. (Memphis to San Jose)	0	Federal Express employee, facing dismissal, crashed plane as part of life assurance fraud scheme.
13.07.1994	Russian Air Force	Kubinka Air Force Base, Moscow	1	Russian Air Force engineer stole a military plane and flew until it ran out of fuel and crashed.
21.08.1994	Royal Air Maroc: Flight 630	Atlas Mountains (Agadir to Casablanca)	44	The pilot, distressed over a break-up, intentionally disconnected the autopilot and crashed the plane into the ground.
19.12.1997	SilkAir: Flight 185	Southern Sumatra, Indonesia (Jakarta to Singapore)	104	The pilot, under financial strain and recently demoted, changed flight controls to crash the plane.
11.10.1999	Air Botswana	Gaborone Airport, Botswana	1	A disgruntled pilot, grounded for medical reasons, made threats and deliberately crashed a plane.
31.10.1999	EgyptAir: Flight 990	Atlantic Ocean – International waters (New York to Cairo)	217	The pilot, reportedly facing demotion, deliberately changed flight controls to crash the plane.
17.07.2012	Canadair	Saint George Municipal Airport, Utah, US	1	A commercial pilot, wanted over a murder, shot himself after attempting to steal a plane.
29.11.2013	LAM Mozambique: Flight 470	Bwabwata National Park, Namibia (Maputo to Luanda)	33	The pilot, facing a string of family tragedies, changed the autopilot settings to crash the plane.
08.03.2014	Malaysia Airlines: Flight MH370	South Indian Ocean – tbc (Kuala Lumpur to Beijing)	239	Plane lost and never traced. The case is inconclusive, but enquiries have considered pilot suicide.
24.03.2015		Mountains near Nice, France (Barcelona to Düsseldorf)	150	The co-pilot, previously treated for suicidal episodes, deliberately crashed plane into a mountain.

TABLE 7.1: LIST OF PILOT SUICIDE CASES, COMPILED BY THE U.S. AVIATION SAFETY NETWORK (2015).

Nevertheless, there are distinct patterns evident across previous cases of suicide and murder-suicide that might be extrapolated to help prevent future tragedies. As Kenedi et al. note, factors associated with both events include legal and financial pressures, occupational conflict, mental illness and relationship stress.[131] Furthermore, there are similarities in the modus operandi, with crashes occurring after the perpetrator is left on their own in the cockpit, for instance when the other pilot leaves to use the bathroom.

As a result of the Germanwings disaster, a number of airlines changed their security protocols to require at least two aircraft crew to remain in the cockpit at all times. This was designed to prevent a suicidal pilot from deliberately crashing the aircraft. However, it paradoxically presented some unintended security flaws. Firstly, an extra person is introduced into the cockpit who might have adversarial intentions. Second, the cockpit door is left open for longer, or opened more frequently, which could expose the cockpit to an intrusion. As a result, many airlines are now reverting to their original security protocols.

Airlines are meanwhile stepping up efforts to detect mental health problems amongst their staff through improving their vetting and monitoring procedures, including aftercare arrangements. However, there are no global binding regulations in place to ensure airlines comply with formal vetting and monitoring measures. Equally, few airlines have in place sufficient support mechanisms for staff experiencing mental health issues.

Likewise, there is more to be done in terms of airlines offering end-of-career employment to their workforce. Pilots are highly specialised in a niche profession and require alternative skills and knowledge to transfer to similarly well-paid and esteemed employment. The provision of appropriate mental health treatment and alternative employment options is at least as important as physical security measures in mitigating the threat of pilot suicide. This will necessarily involve the whole workforce, as some of the signs of deteriorating mental health and associated erratic behaviour are likely to be picked up by colleagues, even if not via formal screening processes.

Incident Summary

On 24th March 2015, Germanwings flight 9525, an Airbus A320-211, flew from Düsseldorf in Germany to Barcelona in Spain. The 34-year-old captain, Patrick Sondenheimer, flew the outward leg and it was agreed that his 27-year-old co-pilot Andreas Lubitz would fly the return journey. The plane, carrying six crew and 144 passengers from 18 different countries, left 26 minutes after its scheduled departure time of 9:35am from Barcelona, but otherwise the journey started uneventfully. By 10:27am, the plane had reached its cruising altitude and the captain asked his co-pilot to prepare the landing checks.

In a cryptic exchange, picked up on the plane's voice recorder, Lubitz replied to Sondenheimer 'we'll see' and 'hopefully'. Lubitz also encouraged the captain to use the toilet several times. Once Sondenheimer had left the cabin, the aircraft immediately left its assigned cruising altitude without notifying air traffic control and began to descend rapidly. Attempts by French air traffic control to contact the aircraft were unsuccessful, whereupon the aircraft was declared to be in distress and a French military jet was scrambled.

The report of the official flight investigation states that after the captain left the cabin, Lubitz locked the cockpit door and disabled the access code.[132] He then deliberately modified the autopilot settings to force the aircraft to descend. Lubitz did not respond to calls from the civil or military air traffic controller, nor to Sondenheimer who was desperately attempting to re-enter the cabin. Automatic alarms systems were by now activated in the cabin. The captain then attempted to batter down the door, possibly with a steel crowbar. At 10:40am, the aircraft crashed into a mountainous ravine at 700km/hr.

131 Ibid.

132 Bureau d'Enquêtes et d'Analyses pour la Sécurité de l'Aviation Civile, 'Final Investigation Report: Accident of the Airbus A320-211, registered D-AIPX and operated by Germanwings, flight GWI 18G, on 03/24/15 at Prads-Haute-Bléone' (March 2016), BEA2015-0125. Available online at: www.bea.aero/en/investigation-reports/ notified-events/detail/event/accident-to-the-airbus-a320-211-registered-d-aipx-flight-gwi18g-on-24-march-2015 [last accessed 17.09.2018].

The report issued a set of recommendations to help prevent future such events, including:

- Regular evaluation of pilots with a history of mental health issues, with conditions applied where deemed necessary such as operational limitations and further psychiatric evaluations.
- Operators to mitigate some of the socio-economic risks related to a loss of licence for medical reasons in terms of how these can impact on a pilot's career, finances and self-esteem.
- Redefinition of the parameters within which pilots could be declared fit to fly while taking anti-depression medication under medical supervision.
- Guidelines of all German health care providers to be amended to balance public safety with medical confidentiality. This includes limiting the legal consequences of health providers breaching medical confidentiality when done in good faith to prevent a threat to public safety.
- Promotion of support programmes for pilots, their familiar and peers, where personal and medical health issues can be shared confidentially and pilots provided with appropriate emotional support.

Suggested Discussion Points:

This incident differs from the other case studies as it deals with the issues of murder-suicide and mental health, as well as the associated question of liability. One of the most challenging aspects of the case is that the medical profession's adherence to patient confidentiality was at the expense of the victims' lives. Some possible questions for discussion are as follows:

- What were the weaknesses in preventative measures at Lufthansa leading up to the incident?
- Assuming the non-disclosure of the relevant medical information was both lawful and morally permissible, could Lufthansa have done more to prevent the crash?
- To what extent should medical confidentiality be upheld when patients are operating critical infrastructure on which the safety and security of others depend?
- Does the new two-person cockpit measure, adopted by a select number of airlines, help to mitigate against the threat of pilot suicide? How does this affect the risk of hijacking?

Case Study 8: Bombing of Daallo Airlines Flight 159, Somalia

Daallo Airlines 159 (DAO 159/D3 153) was an international passenger flight departing from Mogadishu, Somalia on 2nd February 2016. Twenty minutes after taking-off, a bomb was detonated in a suicide attack inside the aircraft, for which the Islamist militant group al-Shabaab later claimed responsibility. The aircraft returned to the airport safely with no casualties except for the passenger, who carried and detonated the bomb. The airport CCTV footage revealed that a senior airport security officer and a long-term al-Shabaab affiliate had handed an improvised explosive device built into a laptop computer to the bomber, after he had passed through security.

Perpetrator Profiles

Abdisalam Borleh - The Passenger

The passenger, who detonated the bomb, was Abdisalam Borleh, a 55-year-old teacher at an Islamic school from Hargeisa (Somaliland). He was travelling on a visa issued by the Turkish Embassy in Mogadishu, which had allegedly received a letter from the Somali Embassy in Ankara claiming he would be working as an advisor for the Turkish Ministry. The Somali Embassy denied its involvement in the visa procedure, suggesting the letter was a fraudulent document. The investigation also revealed that he had been monitored by the Somali federal authorities in the past but was never considered to be dangerous. After the attack, security camera recordings showed two individuals identified as airport workers handing him the laptop in which the explosive device was concealed. The laptop had been delivered to him after the X-Ray security check. Borleh carried it on board and took a seat in the sixteenth row by the window, where he detonated the bomb shortly after take-off. Experts however remained sceptical as to whether Borleh had knowingly or unwittingly committed the attack. This was because the explosion occurred before the plane reached thirty thousand metres altitude, where the bomb would have caused far greater damage due to the differential pressure. Borleh had also detonated the device from the sixteenth row instead of asking to be seated at the back of the plane, which could have destroyed the commands and the elevator. Commentators therefore suggested that Borleh might have been told that he was smuggling drugs.[133]

The Airport Employees

The investigation revealed that two members of the terrorist organisation al-Shabaab, including a senior airport security official (former Security Chief of the Aviation Agency at Aden Adde International Airport) named Abdiwali Mahmud Maow, had plotted the attack. Maow conspired with a long-time al-Shabaab affiliate named Arais Hashi Abdi.[134]

133 Philip Baum, 'Daallo Airlines Bombing: Interview with Captain Vladimir Vodopivec' (2017) in Aviation Security International, Vol. 23, Issue 1. Available online at: http://www.avsec.com/media/files/int01.pdf [last accessed 10.08.2018].

134 Mohamed Olan Hassan, '10 Convicted for Somali Passenger Plane Bomb' (May 2016) in Voa News. Available online at: https://www.voanews.com/a/ten-convicted-in-somali-passenger-plane-bomb/3351953.html [last accessed 10.08.2018].

Compelling documents were found during the investigation, attesting that Abdi had produced the explosive device and masterminded the attack. On 30th May 2016, the two men were sentenced to life in prison by the Somali military court. Arais Hashi Abdi was tried in absentia.[135] Eight other airport workers were sentenced to time in prison ranging from six months to four years for assisting the plot, despite not being affiliated with the terrorist organisation. These included security screeners, a police officer, a porter and an immigration officer. Little is known as to whether these other members of the security staff were coerced to cooperate with co-conspirators or were found liable for negligence. Abdi and Maow were however the only suspects convicted on terrorism charges.

Preventative Measures and Security Systems

Following the incidents, security experts and crewmembers raised several issues relating to local political instability and the lack of reliable security procedures at Aden Ade International Airport in Mogadishu. Approximately 70 passengers, including Borleh, were originally meant to travel on a Turkish Airlines flight scheduled earlier on 2nd February. Turkish Airlines had cancelled the flight in question after receiving an anonymous warning about a bomb two days prior to departure. Officially, passengers were only informed that the flight was cancelled due to the weather conditions. As a result of extra passengers boarding on the Daallo Airlines flight, departure was delayed by twenty minutes, which could explain why the explosion only occurred relatively early into the flight and before the plane had reached a critical altitude.

In retrospect, evidence seems to suggest that al-Shabaab had initially targeted the Turkish company. In an interview, the pilot pointed out that the terrorist organisation had not had much interest in attacking Somali civilians travelling via a local company. Alternatively, Turkish Airlines, who represented one of the main foreign investors in the region, was far more likely to be targeted. Al-Shabaab had claimed an attack against the Turkish embassy on 27th July 2013 and another attack on a beach restaurant located in the surroundings of the embassy in August 2016.[136] At the time of the attack, Aden Ade International Airport had benefitted from significant investments from Turkish Airlines. The company had funded a new building, along with a range of new security facilities. Yet the airport suffered from a lack of centralised security procedure, relying exclusively on the regulations individually applied by the companies. When commenting on his experience flying to Mogadishu for the Somali-owned airline, the pilot of the DAO 159 flight alluded to the fact that this generated additional workload and stress for private airlines' personnel:

> *We don't have any agency there; every company is doing everything themselves: the loading, the distribution, load sheet, documents. And all the time it's fifty degrees outside and there are only forty minutes to check around the aircraft [...] To prevent something [like this] is on the airport. It's not on us.*[137]

Private airlines staff had already witnessed incidents related to drug trafficking and considered Mogadishu International airport a high-risk destination. They reported that it lacked the infrastructure required to meet the security requirements for aviation, with no high frequency communication or meteorology reports and a nondirectional beacon and instrument landing system. Retrospectively, experts also raised concerns about the training of the security workforce. In an interview about the case, a former official from the U.S. Department of Homeland Security and president of 'Implant Sciences' stated that developing countries were still facing significant challenges when 'training and maintaining an effective security workforce'.[138]

135 BBC News, 'Daallo Airlines blast: Somalia sentences two to life in prison' (May 2016). Available online at: https://www.bbc.co.uk/news/world-africa-36411555 [last accessed 10.08.2018].

136 Feisal Omar & Abdi Sheikh, 'Al Shabaab claim attack on Turkish mission in Somalia, three dead' (July 2013) in Reuters. Available online at: https://www.reuters.com/article/us-somalia-conflict-idUSBRE96Q0A420130728? feedType=RSS&feedName=worldNews [last accessed 10.08.2018].

137 Philip Baum, 'Daallo Airlines Bombing: Interview with Captain Vladimir Vodopivec' (2017) in Aviation Security International, Vol. 23, Issue 1. Available online at: http://www.avsec.com/media/files/int01.pdf [last accessed 10.08.2018].

138 Paul Cruickshank & Robyn Kriel, 'Source: 'Sophisticated' laptop bomb on Somali plane got through X-ray machine' (February 2016). Available online at: https://edition.cnn.com/2016/02/11/africa/somalia-plane-bomb/index.html [last accessed 10.08.2018].

The Somali Transitional Federal Government had commissioned a Dubai-based aviation firm that specialised in conflict zones to train 200 local workers in order to meet international airport standards by 2010. The company, called SKA logistics[139], was also in charge of implementing electronic check-in systems and securing access to the Internet for the Somali Police Force, immigration and customs, and the Somali Civil Aviation and Meteorological Agency (SCAMA). In 2013, the Turkish government, who were engaged in the local post-conflict reconstruction process, invested $10 million in a project of renovation intended to increase the airport's 15 aircraft capacity to 60 and build a modern control tower. The project was carried out by the Turkish company Favori LLC[140] and a new terminal, which enabled the airport to double its number of daily commercial flights, was inaugurated in 2015. However, the airport's security infrastructure had only been implemented fairly recently by foreign agencies that were no longer actively involved in the supervision of these procedures. Although SKA logistics had experience working in politically unstable environments, they may not have been fully aware of the particularities of the Somali context. In this context, the professional legitimacy and authority of foreign experts may have been channelled, which would explain why efforts to implement an efficient security culture were unsuccessful.

Incident Summary

Borleh detonated the bomb approximately ten minutes into the flight after the seat belt signs were switched off. The explosion tore a hole in the Airbus fuselage and Borleh immediately fell out of the plane. The flight returned to Mogadishu airport for emergency landing approximately fifteen minutes after the incident. Local authorities, including the Chief of Security at the airport, submitted a report to the pilot in which they suggested that a member of the cabin staff could have unintentionally activated one of the oxygen canisters. The pilot refused to sign the initial report and was invited to stay in Mogadishu along with members of cabin crew until a new report was issued 48 hours after the incident. Somalia's Air Accident Investigation Authority (SAAIA), the National Intelligence and Security Agency (NISA), and the FBI eventually discovered that the bomb had been hidden within a laptop carried onto the aircraft by Borleh, a passenger in a wheelchair. Al Shabaab claimed responsibility for the attack on 13th February 2016, stating that the operation had initially targeted dozens of Western intelligence officials and Turkish NATO forces.[141]

Suggested Discussion Points:

- Could the foreign companies commissioned to train security personnel have fully anticipated the risks relating to the local context?
- To what extent did the lack of trust between stakeholders (airlines, airport staff and/or foreign security experts commissioned by the government) hinder the implementation of successful and sustainable preventive measures?
- Does preventing other forms of insider criminal activities contribute to reducing the risk of terrorist insider threat?
- What kind of preventative measures would allow staff members to identify or report an insider with a high managerial position within the organisation?

139 SKA International Group, 'SKA in Somalia, Somalia Operations'. Available online at: http://www.ska-arabia. com/ska1701/ska-in-somalia/ [last accessed 10.08.2018].
140 Mogadisu Airport Official Website, 'Favori' (October 2013). Available online at: https://mogadishuairport. com/favori/ [last accessed 10.08.2018].
141 Hamza Mohammed, 'Al Shabab claims Somalia plane bomb attack' (February 2016). Available online at: https://www.aljazeera.com/news/2016/02/al-shabab-claims-somalia-bomb-plane-attack-160213130832329. html [last accessed 10.08.2018].

Case Study 9: Greenfield Water Reclamation Plant Sabotage, United States

Perpetrator Profile

Robert Olson had served in the U.S. army from 1986-1989 before later becoming a wastewater plant operator certified by the Arizona Department of Environmental Quality. His employment history from 2001 onward shows that he initially worked for the city of Mesa until 2002, and subsequently worked for plants in Phoenix and Avondale. In 2007 he returned to Mesa to work at the Greenfield Wastewater Treatment Plant in Gilbert, Arizona. According to newspaper articles published at the time, Olson switched back to Mesa to be closer to his home and to spend more time with his family. [142] [143]

Olson passed FBI background checks and his personnel records are said to have shown excellent performance reviews. Olson only received his first reprimand in 2008 for not notifying his supervisor that his replacement for the night had been cited for a driving under the influence (DUI). Around the same time, Olson lost his home in the Mesquite Canyon neighbourhood of Mesa to foreclosure, and a neighbour has suggested that he and his family were then forced to move in with his in-laws.

These setbacks came on top of several health issues. In 1998 Olson had been diagnosed with testicular cancer and had sought out the support of mental health support services. Although the court documents do not report further on Olson's physical wellbeing, they do describe that he was diagnosed as bipolar, personally he claimed to have dual personality disorder.[144] He tried to cope with depression and stress via various medications prescribed to him by a psychiatrist, including Sertraline, which has the potential to cause suicidal tendencies. These tendencies caused Olson to be admitted to a treatment centre twice during 2011. It has also been reported that he possibly abused alcohol and psychostimulant drugs.

According to his own statements, Olson never actively attempted to hide his mental health issues from his employers. The court case shows that between January 1st and April 1st of 2011 several e-mails were exchanged between Olson and the City of Mesa Human Resources department, in which Olson continually flagged health concerns and requested to be taken off the night shift. During March, Olson called his psychiatrist three times, detailing he did not feel well and needed to be seen. Notably, Olson's psychiatrist did not see him, but instead increased his dose of medication over the phone.

142 M. Sakal, 'Court documents describe wastewater worker's frustration' (2011) in East Valley Tribune. Available online at: http://www.eastvalleytribune.com/local/court-documents-describe-wastewater-worker-s-frustra tion/article_5d7d0434-5fd8-11e0-842a-001cc4c03286.html [last accessed 23.08.2018: only available from the US, protected by GDPR in the UK].

143 M. Sakal & G. Groff, 'Mesa worker arrested in disruption at wastewater plant' (2011) in East Valley Tribune. Available online at: http://www.eastvalleytribune.com/local/mesa-worker-arrested-in-disruption-at-waste water-plant/article_78e7a406-5ca2-11e0-9581-001cc4c03286.html [last accessed 23.08.2018: only available from the US, protected by GDPR in the UK].

144 The State of Arizona versus Robert Anthony Olson (Case CR2011-116355-001). The Judicial Branch of Arizona, Maricopa County. A summary of the documents is available online at: http://www.superiorcourt.maricopa.gov/ docket/CriminalCourtCases/caseInfo.asp?caseNumber=CR2011-116355 [last accessed 23.08.2018]. Assisting with this research project the full court case was accessed in person by James Russell, to whom KCL CSSS expresses its immense gratitude. Many of the facts included in this case study are taken directly from these documents.

Next to his health struggles, Olson was becoming increasingly dissatisfied with lack of pay raises, while employee medical premiums and costs of living were growing. He specifically mentioned being angry with the City of Mesa for investing a huge amount of tax-payers money in new spring training facilities for the Chicago Cubs baseball team (presumably instead of investing in employee benefits). The City of Mesa Executive Budget Plan for 2017/2018 shows that Mesa voters approved of this plan in November 2010, and the city issued $104.5 million of tax bonds to support construction and renovation. Significantly, the Cubs training facilities fall under The Enterprise Fund, which is utilised to account for city-owned systems including wastewater.[145]

Incident Summary

On his way into work for the night shift on 31st March 2011, Robert Olson stopped at Walmart to buy several cans of light beer and bottles of 'Mike's Hard Margarita drinks' as well as beef jerky. Either there were no contraband checks at the facility, or Olson managed to bypass them. Around 10:40pm, Olson went on to relieve his colleague on duty, Rod Liebe. Liebe did not report anything out of the ordinary when Olson arrived. With no two-person rule either in place, or being adhered to, Olson was the only employee on duty until the morning hours. Over the next hour, he intentionally began to systematically disable controls and shut off numerous valves to critical components of the water reclamation plant. Some of these components controlled the flow of sewage, preventing it from spilling onto the streets through manholes. Other plant systems were designed to provide treatment to sewage so that filtered water could be re-used for purposes such as irrigating food crops. Olson also turned off wastewater pumps, digesters, and flares that burn off increased methane gas. To mask his actions he disabled alarms, which would have notified other personnel of the malfunctions, and he manually closed valves so that the changes could not be remotely noticed or accessed via computers by other personnel. He also disabled the entry gates to the plant.

Once Olson had completed these actions, he retreated to the top of the Solids Operations Building with a folding chair. There, he watched a DVD and drank approximately three of the beers and three of the margarita drinks. He also took about fifteen psychostimulant pills which he had been prescribed for his depression. Olson stated he did this hoping that drinks and medication would cause him to be brave enough to face what was coming. According to the police reports, one of the immediate effects of his actions was the flooding of the building's basement floor, which was filled with approximately half a metre of raw sewage. In addition, due to the pump and valve manipulations, methane gas was vented into the atmosphere for several hours at a rate of 80-120 cubic feet per minute.

Around 2:30am Robert Olson dialled 911 and contacted the Gilbert Police, notifying them of his criminal acts and his intentions. He told the phone operator: 'I am taking the plant hostage'. He stated that methane gas was being released, which could be ignited and cause an explosion destroying a quarter of the city block. Olson said that the release of the methane gas was his 'failsafe', referring to his impending standoff with the police. He later admitted during an interview that he believed a muzzle flash from a police officer's weapon would ignite the methane and cause an explosion. However, the plant supervisor, Ray Aquallo, as well as city officials, have stated while some form of an explosion was conceivable it would have been highly unlikely and would have posed no serious threat. Olson further stated that he was intending to commit 'suicide by cop'. He was armed with a handgun and five rounds of ammunition as well as a knife, and hoped for a gun battle. Olson later said that his gun was not loaded; he kept it in his backpack and never showed it. He also later stated that he never intended to hurt anyone with his gun. Olson reportedly spray-painted a target on the shirt he was wearing, as well as a bandage on his head, so that the officer would know where to shoot in order to kill him.

145 C. J. Brady, City of Mesa Executive Budget Plan 2017/2018 (2018). Available online at: http://www.mesaaz. gov/home/showdocument?id=22809 [last accessed 02.07.2018].

The Gilbert Police Division along with the Tactical Operations Unit negotiated with Olson and were successful, resulting in his surrender at 4:33am. They interviewed Olson on how and why he had committed the acts. In addition to hoping for a major explosion and sewage spilling into the streets, Olson stated he believed that particulates could have been released into the air, which he thought could cause serious injury to individuals. He wanted to influence the policy or affect the conduct of the city of Mesa management, who operate and maintain the water reclamation plant. Furthermore, he wanted to cause substantial damage or at least cause substantial interruption of utilities. Olson also admitted that he had first started thinking about the sabotage several weeks earlier, and his original plan was to take two particular supervisors at the plant hostage and use them as bargaining chips.

During the questioning Olson gave two primary reasons for his actions: his depression and intention to die, but also his anger toward the City of Mesa management. He told authorities he wanted to show the city that 'employees had power'. Olson also reported his bipolar disorder, stating that he felt a suppressed, angry and aggressive personality emerging. Olson was eventually charged with four counts:

1. Terrorism, specifically being intentionally and knowingly engaged in terrorism, a class 2 felony;
2. Burglary in the first degree, a class 3 felony;
3. Criminal damage, a class 4 felony;
4. Misconduct involving weapons, specifically the use of a handgun in the act of terrorism, a class 2 felony.

Olson was convicted of the 2nd and 3rd count, but not the 1st and 4th. Olson did not receive a prison sentence, but was sentenced to 4 years of probation starting 12th January 2012. He was also ordered to pay $2,003.41, split into $25.00 per month, beginning 1st March 2012.

Olson was granted his probation on 26th January 2012, with the Probation Officer citing that he was 'non-dangerous – non-repetitive'. He had been cooperative and honest with the police and had not resisted. He was educated, worked his entire life and had never had issues with the law. His wife and two children had likewise always been contributing and law-abiding citizens. Olson stated that he was willing to do whatever was required of him and comply with everything to move on with his life. He had successfully completed the Phoenix Interfaith Counselling course in Life Management Skills based on Dialectical Behavioural Therapy. This course included 'Core Mindfulness', 'Interpersonal Effectiveness', and 'Emotion Regulation and Distress Tolerance'. The counselling program was supposedly key in helping Olson reunite with his wife, with whom he had become estranged after his arrest. Olson's mental health case manager reported that he was compliant with his mental health treatment plan. Olson obtained full time employment and paid his Court Ordered Restitution in full. He was also put on different medication, which according to the most recent report is working well.

> "HE WANTED TO CAUSE SUBSTANTIAL DAMANGE OR AT LEAST CAUSE SUBSTANTIAL INTERRUPTION OF UTILITIES"

The Greenfield Water Reclamation Plant itself suffered $60,000 in damages but did not seek restitution. Following the events of 1st April 2011, they immediately fired Olson and asked the court to order him to stay away from the City of Mesa employees and facilities. The Plant is currently undergoing a major multi-million dollar expansion.[146]

146 Capital Improvement Projects, Gilbert Arizona, WW075 / WW114: Greenfield Water Reclamation Plant Phase III Expansion (2017). Available online at: https://www.gilbertaz.gov/departments/public-works/engineering-services/capital-improvement-projects/ww075-ww114-greenfield-water-reclamation-plant-phase-iii-expansion [last accessed 06.07.2018].

Preventative Measures and Regional Context

According to the Preventative and Protective Measures against Insiders Threats handbook published in the IAEA Nuclear Security Series (No. 8), measures that could have been taken to prevent theft or sabotage include:

a. *Identifying undesirable behaviour or characteristics, which may indicate motivations, prior to allowing employees access.* However, in this case Olson passed FBI vetting, despite reporting mental health issues. Although it is not clear which company Greenfield worked with, there are at least two organisations which provide security in the U.S. water industry. A company called InfraGard liaises between the FBI and the critical infrastructure industry on security issues. They have simulated threats to a water treatment site, and there is a record of them providing information on insider threat prevention best practices.[147] In addition, WaterISAC is an organisation that specifically provides security and continuity of service information to the water treatment industry. In fact, one of their analyses cites the Greenfield case, alongside another incident in Georgia, where a treatment plant employee was fatally shot during an altercation with a contractor.[148] However, it has been suggested previously that standard screening, or pre-employment, background investigation in the U.S. can be a relatively ineffective preventative measure[149] as it consists primarily of a review of their criminal record (or absence thereof) and credit history.

b. Limiting access, authority and knowledge, particularly though compartmentalisation of information and areas. In this case Olson had sole and unrestricted access to critical systems and facilities during his night shift on 1st April. Here, protective security measures such as a two-person rule could have potentially prevented this incident.

c. *Regular trustworthiness assessment of an individual's integrity, honesty and reliability.* It would appear in this case that Greenfield clearly never picked up on, or became alarmed by, the changes in Olson's financial situation. In addition, in Arizona, an employer is allowed access to an employee's medical records with their express consent.[150] From the court case, there is no obvious reason to assume that Robert Olson would have denied this access. In addition, psychologists may disclose private information without consent in order to protect the patient or the public from serious harm if, for example, a client discusses plans to attempt suicide. However, Olson's doctor apparently never alerted Greenfield.

d. The belief in a credible insider threat. Either Olson never mentioned his political views, or none of his family, friends and colleagues picked up on or thought it necessary to report his growing discontent with the City of Mesa. Hypothetically, this could reflect the broader security culture at Greenfield, with Olson himself not reporting that a colleague had been cited for a DUI (Driving Under the Influence).

147 K. J. Paloucek, 'The Threat to Our Water Supply' (2017) in InfraGard Magazine. Available online at: https://infragardmagazine.com/the-threat-to-our-water-supply/ [last accessed 23.08.2018].

148 WaterISAC, Assessing Threats and Mitigating Risks (Presentation) (2011). Available online at: http://www.orwarn.org/files/08%20GlazerWaterISACORWARNPresentation[1].pdf [last accessed 23.08.2018].

149 N. Catrantzon, No dark corners: defending against insider threats to critical infrastructure (thesis) (2009). Available online at: https://calhoun.nps.edu/bitstream/handle/10945/4656/09Sep_Catrantzos.pdf? sequence =1 [last accessed 23.08.2018].

150 HealthInfoLaw.org, Privacy and Confidentiality in Arizona (2018). A.R.S. §36-664; A.R.S. §36-125.05; Confidential records; immunity - Ariz. Rev. Stat. Ann. §36-509. Available online at: http://www.healthinfolaw. org/state-topics/3,63/f_topics [last accessed 06.06.2018].

Broader Issues

There are over 16,500 publicly owned treatment works that provide wastewater services in the U.S. and, as touched on, the idea of sabotage of water operations is not a new concept. In 2001 the FBI alerted U.S. water utility executives that they had 'received a signed threat from a very credible, well-funded, North Africa-based terrorist group indicating that they intend to disrupt water operations in 28 U.S. cities [...] The FBI has asked utilities, particularly large drinking water systems, to take precautions and to be on the lookout for anyone or anything out of the ordinary'.[151] The threat was later determined to be a hoax, but security awareness of this kind of sabotage was nevertheless heightened. As a result, the National Infrastructure Protection Center (NIPC) as well as Critical Infrastructure

Protection Advisory Group (CIPAG) were established, and asked the U.S. Environmental Protection Agency (USEPA) and Metropolitan Water Agencies (AMWA) to develop a vulnerability assessment methodology.[152] [153] However, many utility companies indicated they had no desire for security standardisation, and it remains unclear from the publicly accessible reports whether the Greenfield Water Reclamation Plant made (or makes) use of the proposed methodology.

Overall, the reality of insider radicalisation does not appear to take top priority in U.S. Wastewater management. According to the 2015 Water and Wastewater Sector-Specific Plan, which relies on the 2013 Roadmap to a Secure and Resilient Water and Wastewater Sector, the most significant risks to the sector are natural disasters, aging infrastructure (specifically economic implications), and managing area-wide loss of water.[154] Intentionally malicious acts are listed a category lower, at 'high risk'. First priority in the report is to advance the development of sector-specific cyber security resources, second to raise awareness of the 'lifeline' status of water, and third to enhance preparedness and resilience. Similarly, the Water Security Handbook published by USEPA emphasises the response to contamination of water and external terrorism, as opposed to preventative measures and insider threats.[155]

In this particular case, it is also key to note that the funds for systems such as wastewater and electricity in the City of Mesa come from the same source as the Cubs Spring Training Facilities.[156] Spring Training and the stadiums associated with these events have been a historically contested subject in the Mesa area. On one hand, Spring Training is argued to inject a large amount of money into the local economy. They attract over 220,000 spectators, with an average attendance per game of almost 14,000.[157] On the other hand, the Spring Training Facilities bring a huge amount of traffic into a city at a time when traffic is already bad (in spring and summer). As a result, locals can feel disconnected from Spring Training in general and newspaper and blog articles attest to annoyance with the developments.[158] [159]

151 G. P. DeNileon, Critical Infrastructure Protection. The Who, What, Why, and How of Counterterrorism Issues (2003). Available online at: http://www.mrws.org/Terror/Counterterrorism.htm [last accessed 23.08.2018].
152 U.S. Environmental Protection Agency (EPA), A Water Security Handbook: Planning for and Responding to Drinking Water Contamination Threats and Incidents (2006). Available online at: https://www.epa.gov/sites/ production/files/2015-06/documents/watersecurity_water_security_handbook_rptb_1.pdf [last accessed 06.06.2018].
153 U.S. Environmental Protection Agency (EPA), Guidelines for the Physical Security of Water Utilities: American National Standard for Trial Use (2006). Available online at: https://nepis.epa.gov/Exe/ZyPDF.cgi/ 60000RBW. PDF?Dockey=60000RBW.PDF or https://nepis.epa.gov/Exe/ZyPURL.cgi?Dockey=60000RBW.TXT [last accessed 06.06.2018].
154 Homeland Security, Water and Wastewater Systems Sector-Specific Plan (2015). Available online at: https://www.dhs.gov/sites/default/files/publications/nipp-ssp-water-2015-508.pdf [last accessed 06.07.2018].
155 G. P. DeNileon, Critical Infrastructure Protection – The Who, What, Why, and How of Counterterrorism Issues (2001). Available online at: http://www.mrws.org/Terror/Counterterrorism.htm [last accessed 06.06.2018].
156 M. Poletta, 'How Mesa would spend $580 million in utility bonds' (2014) in AZCentral. Available online at: https://eu.azcentral.com/story/news/local/mesa/2014/09/30/mesa-spend-million-utility-bonds/16479979/ [last accessed 06.07.2018].
157 L. Gomez, 'Cubs games account for 5 largest crowds in Arizona spring-training history' (2018) in AZCentral. Available online at: https://eu.azcentral.com/story/news/local/phoenix/2018/04/06/arizona-spring-training-attendance-dips-2018-despite-record-chicago-cubs-games/479668002/ [last accessed 06.07.2018].
158 W. Schutsky, 'Development hasn't sprung up around Cubs' Mesa stadium' (2018) in East Valley Tribune. Available online at: http://www.eastvalleytribune.com/local/mesa/development-hasn-t-sprung-up-around-cubs-mesa-stadium/article_e0619548-15bd-11e8-8dd4-0fe75c5569b1.html [last accessed 06.07.18: only available from the US, protected by GDPR in the UK].
159 M. Sommer, 'Spring Training Stadiums Are a Bad Investment, And No One Cares' (2014) in CityLab. Available online at: https://www.citylab.com/life/2014/01/spring-training-stadiums-are-bad-investment-yet-no-one-cares/8265/ [last accessed 02.07.2018].

Further considering the context of this case, it is possible that institutional discrimination in Arizona was a factor in enabling Olson.[160] [161] The conservative sheriff at the time, Joe Arpaio, has styled himself 'America's Toughest Sheriff' (and published two books under this title).[162] He has said that armed white men, no matter how extremist, are not perceived as a 'threat' while law enforcement concentrates its energies on undocumented immigrants. In line with this, Olson's neighbour commented that 'he wasn't a gun toting radical by no means [...] I'm shocked".[163] Arpaio was sentenced for racial-profiling practices in Arizona and lost his run for a 7th term in 2016, but he was pardoned by President Trump in August 2017 and subsequently announced he would run for U.S. Senate.

Arpaio was not alone in upholding this line of law enforcement in Arizona. In 2010 senator Russell Pearce and Governor Jan Brewer sponsored a controversial anti-immigration bill, requiring local police to enforce federal immigration laws whenever they suspected an individual to be an illegal immigrant, which critics have said in effect legalised racial profiling.[164] Arizona's approach seems to have been endemic to both staff members at the Water Reclamation Plant as well as law enforcement in the area, who may have found it difficult to accept the reality that an educated, local, white man could be a threat.

Suggested Discussion Points:

- How is it possible that Olson was able to take alcohol into work, and what happened to the colleague cited for a DUI? A recent vacancy from Greenfield states that 'due to the safety and/or security sensitive nature of this classification, individuals shall be subject to pre-employment or pre-placement alcohol, drug and/or controlled substance testing as outlined in City policy and procedures'.[165] [166]
- Why was Olson allowed to work his shift alone? Usually critical material or operations require the presence of at least two authorised individuals at all times (the 'two-person rule').
- Why did the City of Mesa or Greenfield Water Reclamation Plant never request to see Olson's medical records, even after he had reported mental health issues to them? In addition, why did Olson's psychiatrist not report the developments in his condition (suicidal tendencies, bipolar disorder) to his patient's employers, considering it was within the law to do so?
- Could national context (the idea that critical infrastructure such as water management is less vulnerable to inside terrorism than other facilities) and regional context (institutionalised racism and the social-behavioural idea that an average, educated, white individual does not necessarily pose a threat) have contributed to underestimating Olson?
- Olson was charged with terrorism, but not sentenced on this count. Do you agree or disagree with this outcome?

160 C. Danielson, The Color of Politics: Racism in the American Political Arena Today (2013). Santa Barbara: ABC-CLIO.
161 S. P. Huntington, Who are We?: The Challenges to America's National Identity (2004). New York: Simon and Schuster.
162 N. D. Rizzi, Joe Arpaio and the Phenomenon of the Toughest Sheriff in America (2016). Thesis presented to the Department of History, Sam Houston State University. Available online at: https://shsu-ir.tdl.org/shsu-ir/bitstream/handle/20.500.11875/61/RIZZI-THESIS-2016.pdf?sequence=1&isAllowed=y [last accessed 06.07.2018].
163 Homeland Security News Wire, 'Wastewater employee charged with terrorism after idling plant' (2011). Available online at: http://www.homelandsecuritynewswire.com/wastewater-employee-charged-terrorism-after-idling-plant [last accessed 23.08.2018].
164 R. C. Archibold, 'Arizona Enacts Stringent Law on Immigration' (2010) in The New York Times. Available online at: https://www.nytimes.com/2010/04/24/us/politics/24immig.html [last accessed 23.08.2018].
165 GovernmentJobs, Water Resources Maintenance Specialist II - Water Reclamation Plant (2018). Available online at: https://www.governmentjobs.com/jobs/1910962-0/water-resources-maintenance-specialist-ii-water -reclamation-plant-3-vacancies [last accessed 06.06.2018].
166 NewportNews, Job Description, Wastewater Inspector – Public work (2018). Available online at: https://www. nngov.com/DocumentCenter/View/3236/Wastewater-Inspector-PW-Wastewater [last accessed 06.07.2018].

Summary

The incidents showcased in this handbook have tried to illustrate some of the different possible paths to radicalisation, leading to insider action. They are a diverse set of cases drawn from different countries and industries, involving the theft of sensitive information or materials and the conduction of violent acts. The focus of this handbook has been on examining the events leading up to the attack or theft, focusing on potential triggers, behavioural changes, and warning signs that could have been identified.

Although none of the case studies in this handbook involve the civil nuclear industry, there is a clear read across that instructors teaching courses in this area should emphasise. In particular with regards to the use of preventative measures at the organisational, regulatory and other levels. Similar security measures that are applied in the industries under study here, such as vetting, behavioural observation and reporting/whistleblowing, are also utilised in the nuclear sector. Through analysing the different case studies various challenges to the effective implementation of preventative measures can be identified and then considered within the nuclear context.

In many of the cases presented there were clear red flags regarding the behaviour of the perpetrators leading up to the incident that could have been recognised and acted upon by those in a position of authority. That they were not is arguably indicative of weaknesses in the security culture within the different organisations under study, in particular with regards to vigilance, personal accountability, and leadership. As such these cases can also provide a useful vehicle for exploring this crucial but relatively new and somewhat intangible concept. Here instructors may wish to utilise relevant IAEA guidance and frameworks for deconstructing nuclear security culture when analysing the different cases.[167] Before asking students, if appropriate, to apply these methodologies to their own organisational contexts.

Finally, it should be noted that the limited number of case studies presented here cannot be expected to provide a complete picture of all aspects of radicalisation, insider threats and preventative measures. It is our hope that this handbook will inspire others to carry out their own research in this area and investigate and develop other relevant cases from their own organisational and national contexts.

167 International Atomic Energy Agency, 'Nuclear Security Culture – Implementing Guide' (2008), IAEA Nuclear Security Series, No. 7. Available online at: https://www-pub.iaea.org/MTCD/Publications/PDF/ Pub1359_ web.pdf [last accessed 17.09.2018] .

Centre for Science and Security Studies
Department of War Studies
King's College London
Strand
London WC2R 2LS
United Kingdom

www.kcl.ac.uk/csss
@KCL_CSSS