World Institute for
Nuclear Security

WINS Special Report Series

Evolving Security Threats and Advanced Security Technologies

April 2018

CONTENTS

FOREWORD TO THE SPECIAL REPORT 4

1. INTRODUCTION 5

2. THE PAST 40 YEARS OF THE TERRORIST THREAT 6

2.1 General Terrorism Trends 6

2.2 Terrorism Involving the Nuclear Sector 8

2.3 Terrorism Against Other Critical Infrastructure 12

3. LOOKING AHEAD: THE NEXT 20 YEARS OF THE TERRORIST THREAT 15

3.1 PESTLE considerations 15

3.2 Future Evolution of the Non-State Nuclear Threat 17

3.3 Other Critical Infrastructure Terrorism Trends 20

4. TERRORISM, TECHNOLOGY AND NUCLEAR SECURITY 22

4.1 The Terrorism-Technology Nexus 22

5. EMERGING TECHNOLOGIES FOR OFFENSE AND DEFENCE 26

5.1 Drones 26

5.2 Remotely Operated Weapon Systems 28

5.3 Cyber Threats and Security 29

5.4 Artificial Intelligence 32

5.5 Enhanced Human Performance 33

5.6 Modelling and Simulation 34

5.7 Biometrics 36

5.8 Cross-Cutting Issues 37

6. SUMMARY AND RECOMMENDATIONS 40

ANNEX 1: NUCLEAR FACILITY INCIDENTS 47

REFERENCES 67

The preparation of this report was supported by the US Department of Energy/ National Nuclear Security Administration under Award Number(s) DE-NA0003251.

FOREWORD TO THE SPECIAL REPORT

WINS organised an International Workshop on "Evolving Security Threats and Advanced Security Technologies" between the 19th and 21st March 2018 in Vienna that was attended by over 50 international specialists. The workshop heard presentations from a wide variety of practitioners who addressed the technologies that could be used and misused in the context of the evolving security threat to the nuclear sector. All of the detailed presentations are available to WINS members on the WINS website.

WINS also commissioned a Special Report that synthesised the key points from the workshop, and put the terrorist threat into perspective. We are grateful to James Halverson, Gary Ackerman and Steve Hoodjer who are professional subject matter experts in the field, for preparing the report that is presented here. We believe the report provides important insights into the subject area and hope that you find it informative and thought provoking. As with the natural world around us, systems, technology and thinking are in a constant state of evolution with strong, competitive forces driving change. If the nuclear sector, and other areas of critical national infrastructure are to remain resilient to attack, then they must remain a minimum of one step ahead of the evolving threats and deploy effective defensive measures.

Dr Roger Howsley
Executive Director

April 2018

The views expressed in this report are those of the authors.

1. INTRODUCTION

In the second decade of the 21st century, we are astonished almost weekly by the announcement of new technological breakthroughs that only a few decades ago seemed the stuff of science fiction. These marvels – in fields as diverse as biology, materials science, robotics and computing – hold the promise of empowering humanity to solve many of its problems, large and small. Unfortunately, they also hold the promise of empowering that small portion of humanity intent on using violence and intimidation against society to further their ideological drives. In the context of nuclear security, one of the chief concerns has long been the threat of attacks by violent non-state actors (VNSAs), especially terrorists, on facilities housing radiological and nuclear (RN) material. Up to this point, nuclear facilities have been among the most hardened infrastructure targets and, fortunately, terrorists have not had much success against them. Yet, we are faced with a natural question: to what extent might emerging and evolving technologies alter the threat equation in favour of the terrorists? As the great inventor and mathematician, Archimedes is reported to have said: "Give me a lever long enough and a fulcrum on which to place it, and I shall move the world." Emerging technologies could very well be lengthening the lever that terrorism can bring to bear against nuclear facilities. On the other side of the coin, the same emerging technologies might also revolutionize the defence of nuclear facilities.

This study therefore examines the nexus between terrorism and emerging technologies, as these concern the nuclear industry. It begins by tracing past and estimating future currents in terrorism, with a focus on nuclear-related targets within the broader context of terrorist attacks on critical infrastructure. The study goes on to discuss how terrorists react to new technologies and the reasons why only a minority of terrorists embrace technological opportunities as soon as these appear. Brief descriptions are then presented of several emerging technologies of interest, discussing the effects these might have on the terrorist threat to nuclear facilities by way of offensive or defensive changes. The study touches on some of the regulatory and legal challenges that dealing with emerging technologies may present, before ending with tentative recommendations for those involved in regulating and securing the nuclear industry.

2. THE PAST 40 YEARS OF THE TERRORIST THREAT

2.1 GENERAL TERRORISM TRENDS

It is vital to recognize that, historically, non-state actors who have violently targeted (as opposed to non-violently protested) nuclear reactor facilities and other pieces of sensitive critical infrastructure have typically not done so strictly in order to compromise the functional viability of these installations. Instead, past cases suggest that many of the actors who target these facilities generally do so, at least in part, because the facilities are public symbols of social order and government legitimacy. Attacks against nuclear facilities then, are often committed by those who intend to engage in the terrorism proper, i.e., attacks involving not only the perpetrators and direct victims, but which are also intended to reach and influence one or more wider audiences. This can be further demonstrated by the sizeable attention terrorists give to threatening nuclear facilities in their planning and public statements, even when the threat is not realistic. Given the prominence of terrorists as a security threat to nuclear facilities, it is important to gain an understanding of trends in modern terrorism and how these might evolve.

In the time since the attacks of September 11, 2001, the study of terrorism has taken on increased urgency, with many experts observing that there have been four distinct "waves" of modern international terrorism:[1]

1. The Anarchist Wave (late 1880s – 1920s)
2. The Anticolonial Wave (1920s – 1960s)
3. The New Left Wave (1960s – 1980s)
4. The Religious Wave (1980s – 2025[2])

This framework does not imply that new terrorist groups with different aims suddenly replace those of the previous wave, but rather identifies transitions from one dominant motivating[3] characteristic to another. Thus the "wave" changes in terrorism have typically entailed a combination of new actors emerging, along with existing actors evolving, to espouse a particular set of social, political or doctrinal ideas.

The systematic study of terrorism as a unique phenomenon dates only to the 1970s, a period which corresponds with virtually all non-state threats to nuclear facilities. This enables us to study the two phenomena together. It will surprise few to find that terrorism has never been more deadly than it is in its present "Fourth Wave" (see figure 1 opposite).

With unprecedented numbers of deaths from terrorism and increased public attention, some have claimed that terrorists themselves have changed fundamentally from the past.

There is little support for this idea, with more convincing explanations being found among environmental changes such as the globalization of economies and societies, the proliferation of potential mass casualty targets and increased terrorist access to secure communications, international transportation and powerful weapons.[4] The history of attacks suggests that greater terrorist access to more sophisticated explosive and ballistic weapons in an increasingly urbanized world, as well as a need to escalate in order to ensure publicity in a noisy media landscape, are the factors most likely to have led to the increased lethality of terrorism in recent decades. In any event, far-reaching underlying developments, like the digital democratization of information, the course of regional conflicts and the shape of the global economy, influence the terrorism threat. Ultimately, violent non-state actors have become emboldened while the societies they target have become more complex and filled with points of systemic vulnerability.

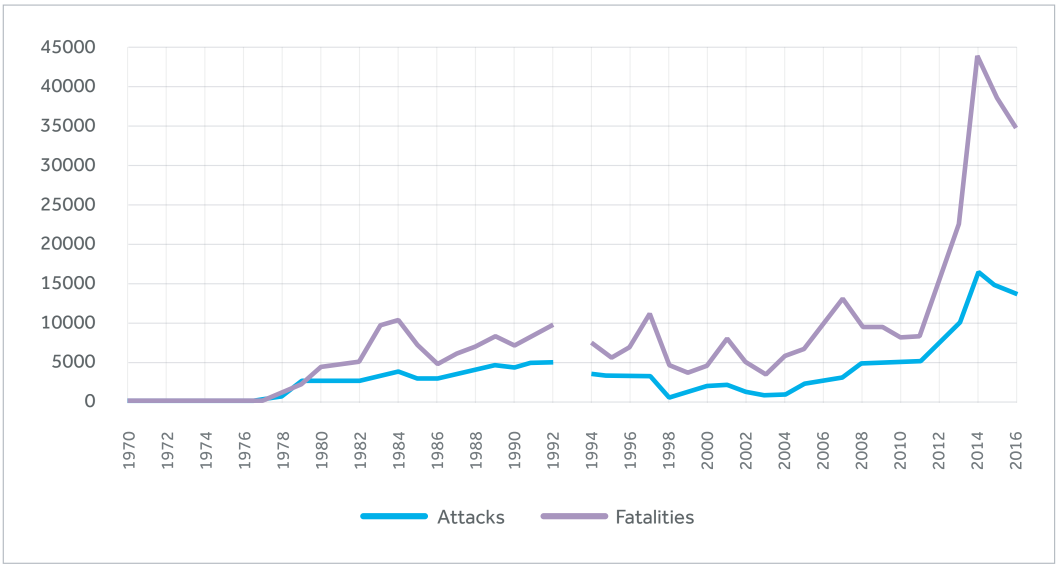

Figure 1: Total Terror Attacks and Fatalities[5]

Terrorism in areas of active conflict is often prolific but overlaps with insurgencies targeting military forces. Some argue that this can distort the overall picture of terrorism, especially when the focus of analysis is on areas of the world not engaged in large-scale conflict. Therefore, although the actions of terrorist actors in conflict regions can be relevant for nuclear threats (thus making Figure 1 above noteworthy), we present Figure 2 below, which shows terrorism since 2000, excluding Afghanistan, Syria, the Democratic Republic of the Congo, and Iraq, which have been areas of major conflict during this period.

As shown, the number of attacks, while still increasing, is considerably lower. Attacks outside conflict zones are also much less lethal with each attack averaging approximately one fatality in many of the examined years. This demonstrates the difference between a large, organized campaign of terrorism as part of a military campaign compared with the more sporadic phenomenon of terrorism as a whole.

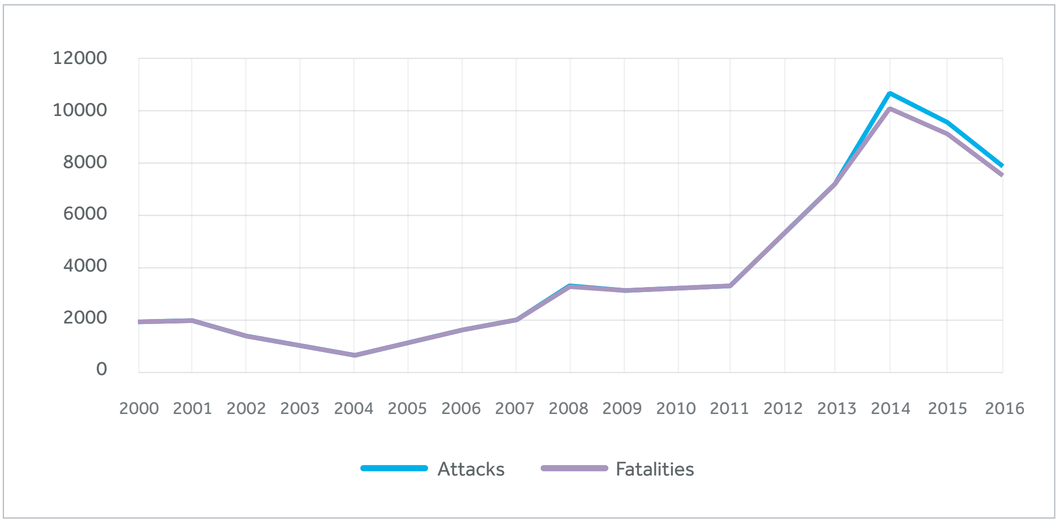

Figure 2: Terror Attacks and Fatalities Since 2000 (Excluding Combat Zones)

2.2 TERRORISM INVOLVING THE NUCLEAR SECTOR

The onset of the nuclear age provided an opportunity for terrorists and other violent non-state actors to seek new heights of psychological or physical impact. Generally, threats of this type consist of the potential for terrorists to acquire a nuclear weapon (or weapons-usable material), as well as the capacity for a VNSA to compromise the safety of a facility housing nuclear material and/or ionizing fission products.

Just as the Cold War and the third wave of “New Left” terrorism were setting in, scholars and security planners began considering how terrorist actors might intersect with nuclear weapons and materials, with the greatest concern being that nuclear weapons could conceivably be used by sub-state groups. Since then, this concern has only grown, as nuclear weapons have spread beyond the post-World War II great powers, and the sporadic demonstrations on the part of terrorist actors that they do have an interest in possessing them.

Significant instances of attempted and apparent non-state actor pursuit of nuclear weapons include the following:[6]

- 1977: The Red Army Faction launch a raid on a U.S. Army installation in Giessen, West Germany, likely seeking to steal, detonate or otherwise damage nuclear weapons housed at the facility.
- Early 1990s: Aum Shinrikyo steal classified nuclear energy operations information from the Japanese government, investigate the purchase of a Russian nuclear weapon and acquire land in Australia from which they intend to mine and enrich uranium.
- Mid-late 1990s: Al-Qaeda investigate a number of means by which they might obtain nuclear material, including black market dealers and the establishment of front companies licensed to handle nuclear fuel.
- 2000-2001: Al-Qaeda's top leadership meet with two nuclear scientists on at least two occasions to discuss the practicalities of acquiring RN weapons.
- 2001-2002: Small quantities of uranium are reportedly discovered in the tunnels under a captured Al-Qaeda facility in the area of Kandahar, Afghanistan.
- 2015: The Islamic State propaganda magazine *Dabiq* publishes claims that they have the ability to readily purchase a nuclear weapon, an entirely unsubstantiated threat, but one that is followed shortly thereafter by the discovery of the group having conducted surveillance of a senior official of the SCK CEN Nuclear Research Center in Belgium.

Though no terrorist actor has yet proceeded past the very early stages of attempts to obtain a nuclear weapon, it is clear that the most ambitious violent revolutionary and apocalyptic/millenarian actors have desired these weapons. Capability has clearly not as yet met this desire, however. Instead, the vast majority of terrorist actors seeking mass casualties have settled for easier and more reliable conventional weapons. Even among actors who have engaged in unconventional weapons plots, most have preferred the relative accessibility of chemical or even biological agents to the complexity of nuclear ones—and evidently also to the uncertainty surrounding radiological weapons.

Agent Type	Number of Plots	%
Chemical	417	76.65%
Biological	97	17.83%
Radiological	52	9.56%
Nuclear	18	3.31%

Table 1: Non-State CBRN Weapons Plots[7]

Perhaps in part because nuclear weapons are the least accessible, the majority of non-state actor plots that have included some nuclear aspect have done so by targeting sites that house fissile material using conventional tactics and implements. A study of 80 incidents (see Annex 1) of high profile plots to breach nuclear facility security finds attempts made by a variety of actors, the most prominent being: criminals (25%), environmentalists (16%), left-wing/separatist extremists (14%), left-wing/anti-nuclear activists (10%) and jihadists (9%).

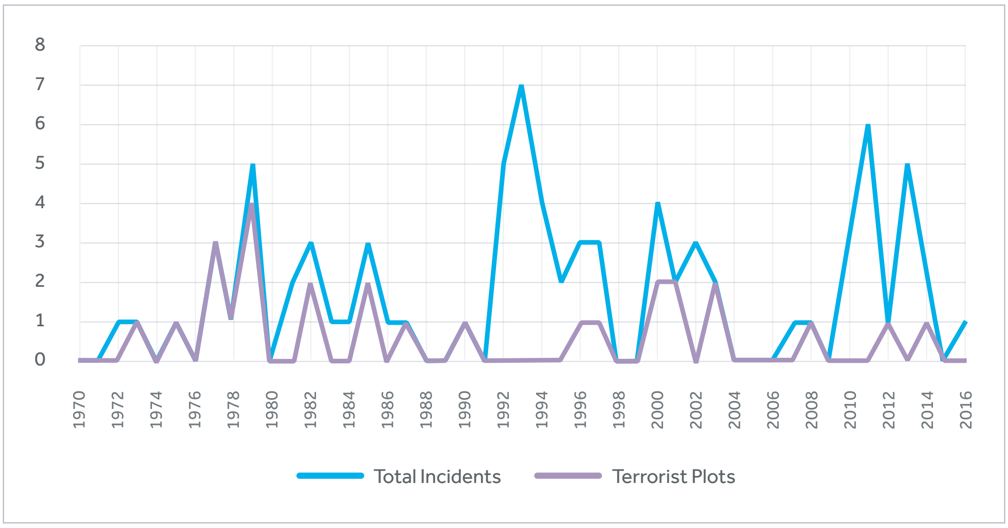

Figure 3: Nuclear Facility Breach Incidents

Only 38 of the cases (48%) included in this set consist of facilities being targeted by actors with violent intentions, of which 26 (33%) appear to constitute actual terrorist plots.[8]

While left-wing terrorist actions were prominent in facility breaches during the Cold War, the years following the collapse of the Soviet Union saw little ideological violence against nuclear facilities. Instead, there were many cases of theft of fissile material from facilities in the former Soviet Union in the early 1990s. The involvement of insiders, which is known to have occurred in a quarter of all included cases, was particularly prominent in this time and place. More recently, organizations falling under the present “Fourth Wave” of transcendent terrorism have been responsible for most violent plots against nuclear installations, but have yet to carry out a successful attack. While few attacks overall have succeeded in terms of causing the harm they intended, many violent attackers (as well as non-violent protestors) have managed to breach the perimeter of controlled areas and a substantial number have engaged in exploits in vital operational areas of facilities.[9]

For most of the past several decades, the most common ideology of terrorists who have plotted to attack nuclear facilities has mirrored that of the concurrent terrorist wave. In fact, all 15 instances of terrorist targeting of nuclear facilities prior to 1990, and in all but two of the evidently terror-driven plots (as opposed to protest or criminal actions) since 1990, the perpetrator’s ideological milieu matches the dominant terrorist ideology at the time. The main distinction observed between terrorist targeting of nuclear facilities in these two periods is that perpetrators in the earlier, “New-Left” wave targeted facilities in their core areas of operation and had considerable success, while the attacks planned by terrorists in the present wave have been directed mostly against far targets in Europe and Australia, and have been unsuccessful.[10]

It appears that trends in nuclear terrorism have generally followed those in terrorism at large. This history may hold some important lessons. Terrorist plots against nuclear targets in the period dominated by left-wing actors yields only one instance—the 1977 Red Army Faction attack on a U.S. Army nuclear weapons installation in Germany—where the attacker appears likely to have desired to bring about some sort of RN hazard. In virtually all other cases, far-left and ethno-nationalist political actors seem to have devised plots that avoided risking criticality or radiological release incidents – and thus potential mass casualties. This was presumably because they wanted to strike a symbolic blow to authority without alienating less radical supporters and sympathizers. In keeping with the general terrorist trend towards greater lethality, more recent nuclear facility attack plots do not show signs of similar restraint with the same consistency.[11] Although there have not been enough cases to provide clear evidence yet that terrorists today pose a fundamentally different threat to nuclear facilities, if the observed parallels between terrorism in general and terrorist nuclear facility attacks reflect a continuing relationship, there is little room for complacency on this point.

2.3 TERRORISM AGAINST OTHER CRITICAL INFRASTRUCTURE

Terrorists across time and ideological space have shared an interest in attacking critical infrastructure (CI) targets, though attacks on CI do not appear to have followed the same "waves" as terrorism more broadly. Instead, ethno-nationalists and secular left-wing groups have continued (at least through 2005) to be the most common source of critical infrastructure attacks.[12] This differs from the case of attacks on nuclear facilities, which have followed along with the larger terror waves. One hypothesis to explain this might be that terror groups locked in struggles with a specific government are the most motivated to attack critical infrastructure but that groups who perceive their cause to have international impact have an added incentive to target nuclear sites. If true, such a dynamic could explain the lack of correlation found between nuclear facility attacks and CI attacks that has been observed in previous research.[13]

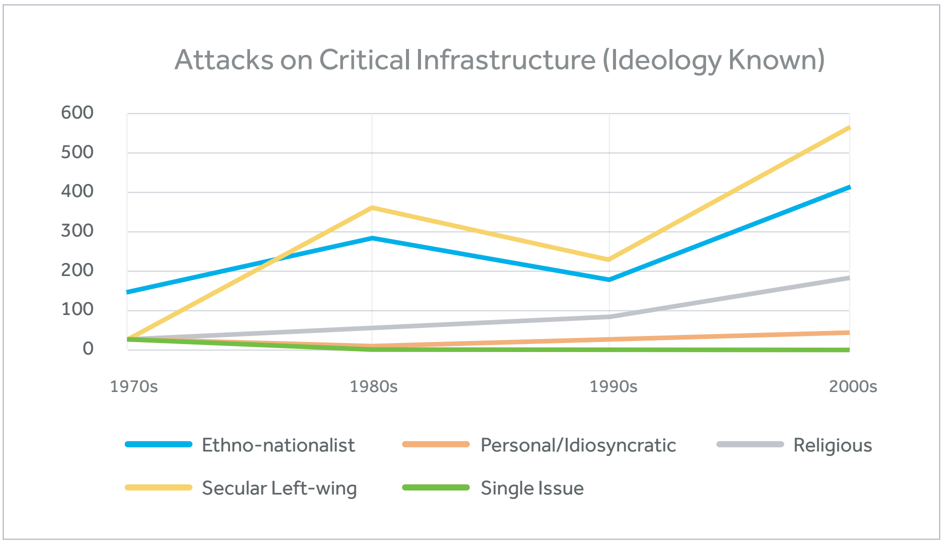

Figure 4: Attacks on Critical Infrastructure

Although attacks targeting other CI will in most cases lack the same potential for psychological impact that might arise from attacking nuclear facilities, CI attacks can serve both instrumental and expressive ends. For instance, they can potentially disable nodes of a target country's essential networks, cause confusion and disruption in its populace and diminish the authority of its government. In many cases, a single attack against a piece of critical infrastructure can achieve all of these effects.

Recognition of the sensitivity of critical infrastructure has in fact been integral to recent terror groups' campaigns of attrition against state rivals, both as a means of disrupting critical systems, and at the very least a way to force security forces into expensive security postures.[14] Even if most attacks targeting CI fail, the occasional major successful attack serves to reinforce the reality of the threat, and force defenders to maintain vigilance at considerable cost. Al-Qaeda documents obtained some time following the attacks of September 11, 2001 stand as perhaps the single most compelling piece of evidence confirming that sophisticated terror groups deliberately seek to impose a combination of compounding effects by targeting critical infrastructure. In the specific case of Al-Qaeda plots against transportation, these were be found to have been deliberately integrated into the organization's strategy in the early 2000s because they could simultaneously paralyze various networks in major cities and kill large numbers of people.[15] Attacks on nuclear infrastructure in particular, however, are likely to be intentionally directed to nuclear targets because of their nuclear characteristics.

One key motivation for targeting CI is the ability to control the number of casualties in an attack. Paradoxically, this makes CI a favoured target for both those groups which seek maximum casualties and those that seek to limit casualties.

Al-Qaeda is a prime example of the former, while the Corsican nationalist group Front de Libération Nationale Corse (FLNC) is representative of the latter. FLNC launched hundreds of attacks against infrastructure targets but killed only a few dozen people overall.[16] We see this in the historical record more generally. In the United States, attacks on CI are "less likely to be deadly and more likely to be highly deadly," as demonstrated in the chart below, although it should be noted that the high lethality figures are largely the result of the Oklahoma City and 9-11 attacks.[17] When considering the threat to nuclear facilities, having a significant social, political or economic impact without loss of life appears to be what many nuclear facility attackers of the "New Left" wave were attempting to achieve, and is the same reason why most environmental activists and anti-war radicals will have no desire to cause radiological releases today.[18]

Total Number of Deaths	Attacks Targeting Critical Infrastructure		Attacks Not Targeting Critical Infrastructure	
	Number	%	Number	%
0	1854	93.3%	534	81.5%
1	90	4.5%	96	14.7%
2-4	31	1.6%	20	3.1%
5-10	4	0.2%	4	0.6%
11-150	4	0.2%	1	0.1%
>150	4	0.2%	0	0.0%
Total	1986	100%	655	100%

Note: Total number of deaths is unknown for 3% of all attacks in the United States

Source: Global Terrorism Database

Table 2: Deaths from Attacks on Critical and Non-Critical Infrastructure Targets

When looking at specific targets within the CI domain, research examining only the United States has found that the greatest number of attacks have targeted commercial facilities (454 cases; 22%) and government facilities (433 cases; 21%), with the energy sector broadly (109 cases; 5.3%) and nuclear power facilities in particular (4 cases; 0.2%) having been relatively less likely targets.[19] With critical infrastructure definitions varying between studies and countries, it is difficult within the limitations of this paper to perfectly measure the field, but we can still discern basic trends.

Looking at updated data and considering critical infrastructure attacks worldwide, with slightly more specific inclusion criteria,[20] attacks on emergency services (22,551 cases; 31.38%), driven largely by police forces being targeted during on-going conflicts in Iraq and Afghanistan, were found to be the most common. Otherwise, government (16,238 cases; 22.59%) and commercial facilities (11,859 cases; 16.5%) remain the most frequently targeted. Attacks on the nuclear[21] and chemical sectors, which draw special attention as low-probability, high-consequence events, are extremely rare by comparison.

Therefore, in their rareness as well as the types of attackers, nuclear facility attacks differ substantially from CI attacks in general. One should thus probably not infer too much from general CI attacks with respect to nuclear facility attacks, although some of the tactical aspects of general CI attacks (especially as these relate to innovation and emerging technologies) might still be instructive.

3. LOOKING AHEAD: THE NEXT 20 YEARS OF THE TERRORIST THREAT

3.1 PESTLE CONSIDERATIONS

THREATENING ACTORS

When surveying the future threat landscape, terrorist groups organized around transcendent, millenarian worldviews will continue to pose the greatest non-state threat, both in terms of their capability to engage in extreme violence and their ideological attraction to mass casualty attacks. Over the course of the recent conflict in Syria, multiple such groups were able to field conventional weapons on a massive scale, engage in unconventional weapons attacks and cultivate impressive cyber capabilities. During this time, the largest of these groups was able to weaponize drones,[22] manage the production of conventional weapons on an industrial scale,[23] produce its own chemical weapons agent and delivery system on a large scale[24] and consolidate cyber assets into a single hacking department.[25] The evolution of the conflict in Syria is, however, likely to lead to a shift within the dominant terrorist milieu from a goal of immediate state-building to one in which terrorists motivated by other-worldly goals see themselves as the flag bearers of a future order that may not come to pass in their lifespan. For defenders, this means facing an opponent that is more fragmented and less capable in conventional terms but also potentially less predictable and more motivated to launch attacks outside of its home region. This could lead to an outbidding strategy in which a number of similar groups compete for leadership of the movement by attempting increasingly spectacular actions, which could include the targeting of nuclear facilities or pursuit of nuclear or radiological weapons.[26]

Ethno-nationalist and separatist groups have historically posed the greatest threat to nuclear facilities[27] and new or reignited ethnic conflicts could trigger instability in various regions of the world. A particularly dangerous subset of VNSAs includes the rise of opposing far right and far left movements in the United States and Europe. It is useful to consider these movements in parallel as their activities typically escalate relative to each other.

Whether and to what extent isolated acts of violence from these groups spill over into threats to the general population remains to be seen.

GEOPOLITICAL & ECONOMIC FORCES

Any evolution on the part of threatening actors will take place in the context of larger shifts in the global balance of power. In addition to disrupting markets and diplomacy, changes in state power dynamics have the capacity to trigger or exacerbate regional conflicts and instability. If competition between major powers takes the form of a trade war rather than a shooting war, the effects may still be of high consequence in terms of undermining stability. A radical pull-back from the current regime of global trade norms could depress the global economy to the point that smaller states, particularly those reliant on one or a few commodities, are plunged into crisis, potentially reversing positive trends towards eliminating poverty.[28]

Such economic instability could increase the flow of migrants from developing to developed countries, straining the resources and social fabric of receiving countries and weakening the human resource potential of the sending countries.[29] Areas of conflict and instability could have far-reaching effects for nuclear security. The security of facilities in zones of instability could be directly threatened by insurgents or warring parties, and instability and economic crisis can divert government attention and resources from radiological and nuclear security in general.

Even short of economic disruption that is globally detrimental, shifts in major markets might disproportionately affect weaker states, potentially giving rise to pockets of instability and conflict, even if top-line measures of economic health appear stable. There is perhaps no region more vulnerable to turbulence of this sort than the Middle East and North Africa (MENA) region. Despite strong growth overall, inequalities in opportunity and wealth, along with high unemployment (particularly among educated youth), can combine with political and ideological movements to drive unrest[30] or violent insurgency.

Even if members of a demographic considered “at-risk,” such as the un- or underemployed do not become drivers of unrest *en masse*, individual members often constitute prime targets for radicalization. This is itself not anything new. However, if rates of educational attainment in technical fields continue to rise in the MENA region without being met by commensurate employment prospects, individuals with science and engineering backgrounds may be susceptible to recruitment by terrorist actors on a much greater scale than before. This could in turn make terrorist actor engagement with unconventional weapons more feasible.

In addition to general increases in unemployment because of factors like nepotism, corruption and economic volatility, the number of educated and unemployed youth might grow significantly as a result of artificial intelligence and robotics advances allowing for the elimination of skilled and unskilled jobs alike.

3.2 FUTURE EVOLUTION OF THE NON-STATE NUCLEAR THREAT

THREATENING ACTORS

Just as in the case of the general terrorist threat, the foremost actors of concern for the near future in the nuclear security context are expected to continue to be actors who purport to act on behalf of theological goals. While the territorial defeat of the Islamic State certainly represents a blow to the threat posed by these sorts of groups overall, the aftermath of the conflict in Syria and Iraq will bring new hazards. The main threats are likely to come from new splinter groups of surviving fighters who plot independently or in cells once they have returned to their countries of origin. Though these actors are virtually certain to be less capable than large territorial entities in Syria and Iraq, they may be more motivated to conduct attacks against very ambitious targets like nuclear facilities, either as acts of revenge or as bids for prestige within the leaderless movement.

The next most likely non-state actor types to target nuclear facilities are nationalist and separatist actors. Actors with ethno-nationalist motivations perpetrated numerous nuclear facility attacks in the “new left” terrorism wave and presently are engaged in numerous conflicts with states in possession of nuclear infrastructure. The most worrisome of these are presently groups that have targeted nuclear facilities in the past.[31] Beyond the ethno-nationalist groups that are well established and presently engaged in struggles with state forces, there appears also to be growing momentum among nationalist and neo-fascist groups in the United States and Europe that may entail intentions to target nuclear infrastructure. Some budding groups in the United States, for example, show signs of rekindling a white nationalist fixation on nuclear weapons first encouraged by *The Turner Diaries*. These groups of “right-wing,” authoritarian extremists thus have some potential to soon become the most likely violent non-state actors to engage in determined targeting of nuclear facilities.

Insider Threats

While there is presently no reason to believe that insider threats to nuclear facilities will rise or fall quickly in coming years, the threat posed by insiders has historically been acute and means of cultivating insiders have only become more numerous in the digital age. Consider five basic types of insiders:

Unwitting: Those that facilitate a breach of security without being aware.

Self-actuated: Those that independently develop and act on intentions to breach security.

Coerced: Those that are compelled under threat to commit or facilitate a breach of security.

Recruited: Those that act in breach of security due to having been incentivized or radicalized.

Infiltrated: Those that obtain access to a facility with a pre-existing intention to breach security.

Digital communication and hacking tools can freely be used to recruit, coerce or use insiders without their knowledge at lower cost and risk than before. The risk of coerced, recruited and infiltrated insiders may be heightened as new nuclear operations commence in or near to regions where violent non-state organizations thrive.

GEOGRAPHIC, ECONOMIC AND TECHNOLOGICAL FACTORS

Historically, attacks on facilities that are near to the attacking group's core area of operations have been significantly more successful than plots that aim farther afield. Therefore, the threat that terrorist groups pose to nuclear facilities might depend upon the degree to which nuclear energy takes root in new parts of the world where sophisticated terrorist organizations are on the rise. Past cases of terrorists targeting nuclear facilities, few though they are, suggest that attacks might be more common and more successful if there is abundant nuclear infrastructure in the same area as the most active terrorist actors of a given period. While terrorists in the developing world would likely find some advantage in conducting facility attacks in familiar areas against new national nuclear institutions, they might also encounter new disincentives.

This could emerge—at least concerning the creation of an environmental radiological hazard—from a fear of alienating local constituents.

Whether a new nuclear project in a small state, or a decommissioning site in a veteran nuclear nation, there are also some developments that have the capacity to create opportunities for adversaries. Cyber weapons, of course, have already been deployed against nuclear facilities and can have impacts ranging from the minor to the catastrophically violent. The fact that the effectiveness of cyberattacks has little to do with how close the attackers are to their target might counteract the previously observed trend of adversaries being more successful in attacking facilities near to their bases of operation. Moreover, the relative anonymity most malicious hackers have enjoyed thus far might lead to the emergence of completely new types of nuclear facility attackers who are neither fervent extremists nor opportunistic insiders but possibly cyber mercenaries or even hobbyists.

Perhaps the most likely source of opportunity for adversaries is fiscal pressure. As the nuclear sector adapts to compete with inexpensive natural gas and maturing renewable energy technologies, not only will security budgets be under greater scrutiny, but altogether new facility designs will be sought. Both these factors could potentially result in novel security challenges that are faced by newly austere security forces. Other potentially consequential dangers, although harder to predict accurately, are factors like natural disasters or large scale armed conflict putting nuclear facilities at risk (whether inadvertently or deliberately). In these circumstances, there is of course the potential for security to be compromised in the confusion and disruption following the event. However, equally important is the increased possibility that adversaries will perceive that vulnerabilities exist, which might encourage additional attempts to attack a nuclear facility.

Serendipity and the Demonstration Effect

The chance appearance of a significant opportunity to attack or otherwise compromise a nuclear facility, or at least the perception that such an opportunity has appeared, could stimulate a large-scale plot against a nuclear facility. In the worst case, such an attack aim to deliberately and demonstrably release radiation from a facility. Moreover, if such an attack is at least partially successful and achieves considerable social and political impact—or is perceived to otherwise further the goals of the attacking actor—interest in attacking nuclear facilities amongst all sorts of adversaries might increase sharply. Conversely, if such an attack is attempted but its impacts can be limited, with the perpetrators killed or apprehended rapidly, interest might decrease and for some time afterwards terrorists might consider the targeting of nuclear facilities to not be worth the trouble.

3.3 OTHER CRITICAL INFRASTRUCTURE TERRORISM TRENDS

THREATENING ACTORS

The increasing trend of unsophisticated, low-tech attacks[32] may indicate a different type of risk being posed to many sectors of CI. This will consist of more self-actuated individuals (often referred to as "homegrown" extremists) seeking softer targets against which unsophisticated attacks can be launched.[33] However, given the historical attraction of terrorists to CI, this threat should be expected to shift focus rather than diminish outright. While the presently dominant wave of terrorist actors are likely to remain the most threatening violent non-state actors generally, the historical prevalence of separatist and ethno-nationalist actors in critical infrastructure terrorism specifically underlines the potential for nuclear-related threats to emerge from a variety of terrorist milieus.

Three trends are likely to be key to the evolution in the terrorist threat against CI: an increasing threat to the energy sector, increased cyber-attacks, and the use of infrastructure targets by violent organizations for financial gain.

TARGETING OF ENERGY INFRASTRUCTURE

While attacks on energy infrastructure have not previously been common relative to other sectors, threats to this sector have increased in recent years. Information from the Global Terrorism Database shows greater than 2.5 times more attacks on energy infrastructure in the current decade than in the decade of the 2000s. The Energy Infrastructure Attack Database records different numbers due to variations in methodology but confirms the overall trend, noting a sharp rise in attacks since 2004.[34] Much of this increase is due to on-going fighting in particular regions, since attacks on oil production are related to conflict duration and intensity.[35] Attacks on oil and gas could spill over into new areas following patterns of new exploration and development. The transport of liquefied natural gas in the Arabian Gulf adds a new vulnerability to long-standing state and non-state threats to shipping in the region,[36] while new gas fields in the Eastern Mediterranean could be a new battleground in a renewed Arab-Israeli conflict.[37] The recent Houthi attack on a Saudi oil tanker as part of the on-going conflict in Yemen should serve as a reminder of the continued VNSA interest in targeting this sector.[38]

CYBER ATTACKS

VNSAs that launch physical attacks against CI and hackers who perpetrate cyberattacks often have very different motivations and organizational characteristics, so thus far incidents of offensive "cyber terrorism" have been limited.[39] However, with the growing connectivity within certain CI sectors and the growing cyber capabilities of VNSAs, this is likely to become a growing threat. Most alarmingly, while cybersecurity in certain elements of CI such as power grids is fairly robust, upgrades to defence may not be keeping pace with the threat.[40] At the present time, it is more likely for state actors to use cyberattacks to disrupt a rival's CI as the nature of cyberattacks makes attribution difficult and is unlikely to trigger a military response. Moreover, terrorist groups usually want to be recognized for their attacks so as to be sure that they serve as a platform for their cause and often seek more tangible violence to be on display in their attacks than can be achieved via cyberattacks. An offensive cyber strategy would be more appealing to a terrorist group which also seeks a long-term campaign of disruption, perhaps seeking, as some recently prominent terrorist actors have, to inflict a number of small defeats upon a target society in order to drain its resources and heighten its fear. With computer science and coding skills becoming more prevalent (including the rise of "cybercrime-as-a-service"[41]), a cyberattack may not come from the usual suspects of well-resourced groups but rather from a new or previously unknown adversary looking to make a large statement at low cost.

VNSA CAPTURE AND OPERATION OF CRITICAL INFRASTRUCTURE

A third emerging trend is the potential for VNSAs to capture and control—rather than simply to destroy—critical infrastructure. In one sense, the attacks of September 11, 2001 involved the capture and use of critical transportation infrastructure as a weapon. A more recent trend in the commandeering of CI by terrorists, however, entails the capture and operation of commodity producing infrastructure. The most dramatic instance of this is the seizure by terrorists in 2015 of oilfields in Iraq. These terrorists were estimated to be receiving as much as half a billion dollars annually from these oilfields.[42] In the same period, these terrorists also controlled numerous dams and used them to control the flow of water to unassimilated populations. While some water handling systems were attacked outright or were poisoned, the preference of the terrorists appears to have been to leave them intact and assume control of their operation.[43] Given the difficulty in capturing and holding assets, this strategy is likely to only enter into the planning of sub-state actors with considerable combat capacity and the desire to hold their own territory. Even so, the isolation and value of energy, transportation and water CI assets in many parts of the world make it possible for smaller violent non-state organizations to attempt to gain at least temporary control of certain CI. In the case of nuclear facilities and other power generation infrastructure, the complexity and expense of operation fortunately prevents terrorists from obtaining similar benefits from commandeering a plant. The only profit motive likely to prompt nuclear facility attacks remains acquisition of nuclear material.

4. TERRORISM, TECHNOLOGY AND NUCLEAR SECURITY

4.1 THE TERRORISM-TECHNOLOGY NEXUS

Emerging technological advances – ranging from 3D-printing and gene synthesis to machine learning and drone swarms – hold the potential for generating new levels of asymmetric harm. There are therefore understandable concerns that these technologies will be exploited by terrorists. However, the path from the appearance of a new technology to terrorist use thereof is not a direct one. In order for an emerging technology to constitute a threat, any terrorist must pass through three "gates": first the terrorist must become aware of the technology's potential utility, it must then make a deliberate decision to pursue adoption of the technology, and – last but certainly not least – the terrorist must successfully acquire and implement the technology in its tactical operations. In today's information-saturated environment, for all but the most closely held military or industrial technologies, we can pretty much assume that terrorists will quickly become aware of emerging technologies. However, passing the second and third gates is not so simple.

With respect to the second gate. The decision to pursue emerging technologies, it is fairly well established that most terrorists, most of the time are tactically conservative and imitative,[44] preferring to stick with what works or at least to emulate what has worked for others. This is partly because terrorists usually have limited resources and are harried by security forces, and because they generally seek to minimize uncertainty, complexity and cost. The process of researching, acquiring and implementing a new technology with an unreliable track record in terrorist operations is thus viewed by many terrorist planners as a risky investment. The main reason why most VNSAs do not innovate tactically, however, is that they do not need to. There are still plenty of "soft" targets available that are highly vulnerable to guns, bombs and vehicle ramming – the most traditional and accessible tools of the terrorist trade.

While terrorists will therefore not seek to use novel or advanced technologies in the majority of their operations, many terrorist organizations do occasionally innovate technologically. A limited number even embrace technological advances enthusiastically. What might prompt them to do so? To answer this question, it is useful to begin with the fundamental driver of innovation: a perceived gap in performance between what is desired and the status quo, a gap that cannot be addressed with existing means and methods.[45] We can now examine a handful of ways in which such a perceived performance gap might arise for terrorists,[46] particularly in the nuclear context.

1. *Existing methods of attack are viewed as being incapable of achieving terrorist operational objectives*. Despite some remaining vulnerabilities, nuclear facilities and materials are, generally speaking, among the world's best protected targets. For terrorists targeting the nuclear sector, new technologies (whether of the digital or physical sort) might be regarded as necessary in order to circumvent existing defences. Also, as defences around nuclear facilities improve, this perceived necessity might grow.

2. The group or individual possesses specific ideological or idiosyncratic goals that motivate them towards innovating technologically (in general or towards a specific technology or advanced weapon). Often referred to as 'techno-fetishism,' this can be a significant motive for some VNSAs to pursue WMD in general and nuclear weapons in particular, as seen in the case of Shoko Asahara of Aum Shinrikyo. It is therefore a logical next step to suppose that the same tendencies that drive some terrorists to pursue nuclear or radiological weapons in the first place might in turn prompt them to use other sophisticated technologies to acquire nuclear weapons or RN materials.[47]

3. *Technological innovation for reasons of status and competition.* If there are rivalries either within a terrorist group or between terrorist groups, the prestige that many people believe to go along with using advanced technology might provide an attractive avenue for parties wishing to distinguish themselves from competitors.
4. *The group possesses an extremely high level of resources, allowing for extensive weapons research and development programmes.* Hezbollah and the Provisional Irish Republican Army are two examples of large, well-resourced terrorist organizations that in the past were able to maintain multiple research and development efforts, while continuing to employ traditional weapons.
5. *Costs associated with adopting new technology are lowered.* As technologies mature, they become more reliable, accessible and commercialized, making their adoption by terrorists less of a gamble. The same outcome can result if a terrorist group gains relevant technical expertise, e.g., if it recruits a new member with advanced engineering skills.

An incomplete list of additional factors that can make the decision to pursue a new technology more likely includes: (1) a high tolerance for risky endeavours, (2) the presence of internal or external champions of a particular technology, (3) having existing expertise with a similar technology, as well as (4) various aspects of the technology itself, such as how easy it is to try out, transport, and use. Moreover, once a given technology has been used by other VNSAs and has been shown to be effective, there is a "demonstration effect", where the tendency to imitate takes over and other VNSAs become much more likely to embrace the technology.

Turning now to the third gate, there are a number of factors that can facilitate the successful adoption and use of a new technology. These include, but are not limited to: (1) the complexity of the technology itself and the amount of knowledge needed to adopt and utilize it, (2) having a safe haven in which to operate, (3) possessing an institutionalized research and development (R&D) unit, (4) having access to both clandestine and commercial supply networks, (5) enjoying state sponsorship, and (6) having a learning culture that can engage in iterative development. While it is rare for any one group to have all of these attributes, there have been – and continue to be – several terrorist organizations that at least during some stages of their development possess many of them. Examples are as varied as ISIS, the Provisional Irish Republican Army (PIRA), Lebanese Hezbollah, FARC in Colombia, the Tamil Tigers of Sri Lanka, Al-Qaeda (both the core and affiliates such as Al-Qaeda in the Arabian Peninsula and al-Shabaab), the Basque ETA, HAMAS, and the Japanese Aum Shinrikyo. The demonstration effect also plays a large role at this stage.

The incorporation of advanced technologies into terrorists' repertoires is not a new phenomenon; as early as the late 19th century, anarchists enthusiastically embraced dynamite as a 'gift of science'.[48] More recently, one of the most recognizable examples of terrorist adoption has been the regular inclusion of new technologies into triggering devices for bombs. These have included mercury tilt switches, the use of barometric pressure sensors for detonating airplane bombs, and a wide variety of common household transmitters (such as electronic garage openers) for the purpose of remotely detonating IEDs.

Beyond weapons, terrorists have also adopted various enabling technologies, especially the adept use of social media for propaganda, recruitment and even training. Lest one believe that terrorists can only employ "off-the-shelf" technologies, there have been several cases where "despite being forced to operate clandestinely and facing the pressures of security forces seeking to hunt them down and neutralize them, at least a subset of VNSAs have shown themselves to be capable of some genuinely impressive feats of engineering", including the development of sophisticated mortar systems and the construction of fully-equipped submarines.[49]

It would be inaccurate to represent emerging technologies as only empowering terrorists and other adversaries; many technologies, from magnetometers at airports to satellites that can intercept communications, have been used by security forces to detect or interdict terrorists and their operations. The static and often reactive tendencies of defence, however, mean that when scanning the horizon, advances on the defence side often seem incremental and slow to emerge when compared to the range of conceivable attack methods. In the nuclear space, by contrast, where security is generally higher than average, more of the advantage belongs to the defender than in other contexts, requiring attackers to consider a wide range of methods of attack that may or may not be practical or effective.

It must also be recognized that many emerging technologies display dual use characteristics: the same technology can facilitate both the counterterrorist defence and the terrorist offense. A simple example is synthetic biology; this technology can be used to design new treatments or prophylactics for a variety of diseases, but could also be leveraged by asymmetric adversaries like terrorists to create new pathogens that circumvent existing treatments. Precisely where the balance of benefit lies is dependent on each case. Adoption by both sides (terrorists and defenders) of such technologies might also result in an offensive-defensive co-evolutionary dynamic, where both sides iterate technologically in order to outdo the efforts of the other party. This dynamic is ubiquitous in nature and is a key driver of evolution in general. As the famous anthropologist Harry Turney-High once stated: "[t]he offense thinks up new weapons or improves the old ones so that the defence's genius must think up new defence or be crushed out of existence. There is nothing new nor old in this. The entire history and prehistory of weapons is summarized in this cycle".[50]

5. EMERGING TECHNOLOGIES FOR OFFENSE AND DEFENCE

Having provided context for terrorist use of technologies, we can now turn to an analysis of how the above factors might come into play with a broad range of today's emerging technologies. This section introduces seven emerging technologies that were discussed at the WINS workshop in March 2018 and discusses how they might affect nuclear facility security. It then touches on two cross-cutting issues that apply to all of the technologies mentioned.

5.1 DRONES

Unmanned Aerial Systems (UAS) have proliferated in a number of martial and industrial applications, as well as across civilian society. Recently, however, UAS systems have also found a place in the arsenals of VNSAs. The scope and success of the Islamic State group's UAS program[51] is but the most prominent of many cases,[52] which indicate that combatants in any future conflict, be they state or non-state actors, are likely to employ armed drones.[53] The use of unmanned aerial systems by non-state actors in combat, however, signals possible future use against civilian targets as well, particularly against otherwise secure sites like nuclear facilities that are hardened against more conventional means of entry.[54] Against such facilities, UAS platforms could be used to conduct reconnaissance,[55] to spoof, distract or desensitize security forces,[56] or even to deploy explosives and other harm agents.[57]

Outside of active conflict zones, UAS presently constitute what security experts classify as a “niche threat”. These constitute novel threats that may force defenders to change their approach and possibly initiate major security adjustments.[58] Outside of battlefield applications, terrorists who have experimented with UAS to date have often chosen not to use them in attack, instead relying on more conventional weapons. This suggests that successful execution of UAS-borne attacks is still difficult enough to restrict the use of this tactic to actors with a particular technical aptitude or specific need for the technology.[59] A terrorist determined to attack a nuclear facility in particular could be among those actors who have a specific operational need for UAS in terms of their ability to provide a low-cost means of defeating robust ground defences.[60] As commercial UAS become more capable, user friendly and widely available, it is possible they will become a standard component in the terrorist toolkit.[61] The appeal of these systems will probably also grow as autonomous flight and swarming technologies become more available. These have the potential to make UAS attacks more potent, easier to conduct and more difficult to counter.[62]

Increasingly, regulations are being introduced to limit where UAS can be operated relative to sensitive spaces like nuclear facilities. While this legislation is necessary and is expected to be expanded in the future, it will need to be enforceable with active measures. A series of UAS overflights of European nuclear facilities in 2014 were technically illegal, but the vehicles proved difficult to track and the perpetrators were never discovered.[63] This case and sporadic similar occurrences since then have demonstrated the difficulty of identifying, attributing, and neutralizing UAS intrusions. Field-ready countermeasures against UAS attacks have only recently begun to emerge, but a number of kinetic and electronic options have emerged from efforts to counter the use of UAS on the battlefield. These systems are designed primarily for battlefield use but may also suit the needs of nuclear facilities.[64]

Currently, methods of early detection of unmanned aerial systems using radar, acoustic sensing and passive RF analysis are all being investigated. These early warning systems will soon allow for quicker and more careful deployment of countermeasures, although it is as yet unclear which countermeasures should be deployed. Jamming of control signals being sent to UAS platforms is an effective option but can be defeated with the use of pre-programmed or otherwise autonomously functioning platforms. This means that the development of kinetic or directed energy systems that can physically disable the vehicle will likely be required. Although such weapons are actively being designed for battlefield use, in the nuclear security context they will need to be integrated with existing security systems, deployable near civilian spaces and also cost effective.

One potential measure for addressing the counter-UAS problem as well as other security needs may actually be the UAS itself. Defenders' UAS could deploy netting or other kinetic measures against intruding drones or serve as perimeter roving platforms for additional cameras and sensors. The greatest benefit of UAS used in the defence is likely to be the greater visibility and awareness that they might provide of the wider owner-controlled areas, where these platforms can introduce more persistent situational awareness and keep human security personnel from venturing into exposed positions.

5.2 REMOTELY OPERATED WEAPON SYSTEMS

The most significant potential impact of remotely operated weapons systems (ROWS) on nuclear facility security is their employment as defensive, force multiplying sentries. A small number of nuclear facilities in the United States have already implemented ROWS systems, primarily as a means of maintaining or enhancing defensive firepower while shrinking the human security force and ultimately cutting costs. Although early varieties of these systems were susceptible to being disabled by sniper fire, newer design features ensure that the weapon and sighting systems are only exposed to small arms fire from positions within the ROWS' line of fire. These systems have also become more resilient to damage or obstruction, as they can be targeted using surrounding camera systems at a facility in addition to the weapon-mounted optics package. The American built versions of this technology are operated by human security personnel on-site but employ a "two key" firing system where both the operator and an off-site manager must approve the firing of the weapon. While the second party verification for firing serves as a safety feature, it could, at least in theory, also be security risk, as facility defence could be compromised by interference at the off-site location or with the communication link.

Russia is also said to have developed robotic sentries for nuclear weapons sites, which may have the capability to function without human participation.[65] Given the clear dangers involved and the sensitivities of Western publics and policymakers, it is unlikely that Western nuclear security institutions will do the same with fully autonomous weapons. That said, more enhanced human-machine teaming is likely to be explored as a "third offset"[66] approach to nuclear security. Robotic sentries and automated systems could improve the reaction time and efficiency of guard forces while remotely operated systems can operate in potentially contaminated environments.[67] As such systems are rolled out, there must be a corresponding focus on protecting their operating software. Cyber infiltrators could, at least in theory, gain access to control systems and change the parameters of who is allowed in a given area and who is considered a threat. In this way, an adversary could combine a cyber-attack with a physical insider or external intrusion in order to facilitate theft or sabotage.

On the offensive side, the ongoing conflicts in Iraq and Syria have served as a laboratory of innovation in many weapons domains. While receiving less attention than UAS, a large number of creatively designed ROWS were devised, produced, and employed in-theatre by combatants on various sides of the conflict. Some of the systems were similar in design to tele-operated sentries employed by advanced militaries but improvised with available weapons and parts.[68] Many used mobile firing platforms ranging from toy radio-operated trucks upon which a rifle was crudely mounted, to homemade tracked vehicles capable of bearing larger weapons.[69] Still others were essentially remote-controlled bombs modelled (perhaps intentionally) after the World War II-vintage “Goliath” remote-controlled anti-tank bomb.[70]

The level of threat ROWS will pose to nuclear facilities in the near future is unclear. Terrorist and insurgent ROWS in Iraq and Syria saw mixed success, usually being of greatest use in static defence applications.[71] Furthermore, as demonstrated in other contexts, VNSAs are not always able to replicate the success of advanced weapons development programs outside the context of sustained combat in a controlled or contested region.[72] The greatest benefit to an attacker outside an immediate conflict zone might be to employ mobile firing platforms as force multipliers in support of a ground attack. If one were to speculate regarding possible operational deployment in the nuclear context: while attackers would need to deploy rather conspicuous weapons systems essentially on-site (perhaps including some final assembly), a skilled adversary fielding a limited number of human operatives could in theory use remotely-operated rifles to overwhelm a limited guard force employed at an isolated nuclear facility or use smaller remote controlled systems to “flood the zone” with targets and divert defenders from the main attack effort.

5.3 CYBER THREATS AND SECURITY

Cyber security presently falls far short of being able to offer assurances that are anywhere near as comprehensive as those expected from the physical security measures in place at nuclear facilities and this comparison in part underscores the potential vulnerability. That is, while a physical attacker will first encounter a guard force trained to observe for and respond to threats, a cyber-intrusion may be encountered first by an operator who is inadequately trained to deal with security breaches.

Cyber security at nuclear power facilities and other complex industrial sites varies considerably; unlike physical security, where the design-basis threat serves as a framework for designing and implementing security measures, there are no universally agreed-upon standards – either in regulation or industry practices – for cyber security.

As a result, security arrangements may vary widely between countries or even facilities within the same country. Some defences are excellent while others may be marginal at best. Sharing best practices and improving training accordingly would be an important step in improving cyber security, but this would require competing companies (and sometimes governments) to be more willing to share proprietary knowledge for the betterment of the industry as a whole.

Up to this point, the defensive side of cyber security at nuclear facilities appears to have been able to protect against attacks. There have been numerous attempts at cyberattacks on facilities but few successful breaches. However, a problematic component of this problem is simply the result of the rate at which cyber weapons evolve and redefine what might be vulnerable. The growing number of attempts combined with successful breaches in other well-protected domains, including finance and government, serve as a warning that current defensive efforts cannot be assumed to be sufficient in future.

One part of the problem comes from the observation that nuclear facilities contain tens of thousands of digital components, designed and installed over the course of decades by various vendors and with differing versions of software.[73] Given these conditions, full-scope cyber threat assessments (i.e., considering every potential permutation of attack vector and target component in a facility) are challenging to say the least. In other cases, the movement towards standardizing and digitizing components creates more vulnerabilities. If an attacker can exploit one networked piece of software that is widely used, then multiple sites are at risk from the same attack. In such cases, returning to analogue systems may be an option to consider.

Another risk is in the nature of cyber security departments. Security is often thought of as a separate piece, which is added to a facility operation, with cyber security added onto that. Often, security departments do not have the required experience in managing complex industrial systems that are necessary for cyber defence.

In addition to bolstering firewalls and updating software, the task of making systems less vulnerable to infiltration in the first place requires that cyber security become part of the broader safety/security culture. It might be that trained engineers who understand the complex digital systems well but have previously focused on safety or operations, will now need to work together with security personnel to protect these systems from cyberattacks.

Defensive measures will accomplish little if personnel are not sufficiently aware of the threat to avoid inviting it in.[74] As part of this shift, the job of improving cyber security then must include the development of systematic methods for prioritizing nodes of concern within a facility's cyber structures, grouping similar systems to ease the analytical burden and prioritizing attack vectors to protect against. Even at the point that satisfactory assessment measures can be developed, however, the challenge of implementing protective measures is no simple matter – the tasks of preventing, detecting and stopping attacks are not trivial.

Accepting that the possibility of cyber intrusion will not be eliminated completely, the challenge of intrusion detection and response must also be considered. Given the potential for there to be only minutes or seconds between the first opportunity to detect a cyber-attack and the point at which it has taken effect, increasingly "smart" automated systems are also being devised to actively attempt to block infiltrations as soon as they are detected. Detection of intrusions are necessarily automated functions that presently are being enhanced with the use of AI machine learning systems like those discussed in the section below. As defensive AI systems develop, so too are AI systems for attack expected to mature, likely leading to more persistent attack attempts and cyber skirmishes between probing attack AI systems and defensive AI systems that play out without any direct human involvement.

Cyber attackers are also likely to seek innovative physical means of gaining access to digital systems, including the deployment of unmanned aerial systems to jump air gaps. These platforms might not only allow for hackers to penetrate Wi-Fi networks or wireless computer peripheral connections at secure sites more discretely and at lower person risk[75] but could also conceivably be a means of introducing imposter wireless networks into secured environments. Given that most cyber-attacks (other than Denial-of Service and Brute Force attacks) are dependent primarily on the skill of the hacker rather than on complex or expensive equipment and are difficult to attribute, they represent a technology that could make attacks against nuclear facilities much more common and likely to be initiated by a wider range of actors.

5.4. ARTIFICIAL INTELLIGENCE

Although artificial intelligence (AI) once referred more strictly to man-made systems with the ability to replicate or approximate the autonomy, creativity and self-awareness that human and other advanced animal brains are capable of, the term is now used more broadly to refer to a variety of less advanced computerized data mining and machine learning technologies. The primary utility of these technologies at present is in comparing, sorting and tagging vast quantities of information at speeds far beyond what any human is capable of. Such tools can be designed and trained to prioritize or otherwise organize the ways in which a system presents data to human eyes, perhaps identifying particular characteristics or patterns in data. A human analyst can then engage selectively with information that is more likely to be of use.

Within a nuclear facility, particularly a reactor facility, systems like these can serve vital functions in the monitoring of multiple persistent streams of safety data throughout a plant. However, these systems also have substantial, as of yet generally untapped, potential to enhance security, particularly in the cyber domain. Given that cyber and computerized industrial systems have made it possible for cyberattacks to compromise physical systems in ways that are either too stealthy or quick to be caught by a human monitor, automated sentinels that can detect anomalies across different systems are increasingly necessary to identify cyberattacks in time to prevent or mitigate their impacts.

As these kinds of AI systems become more capable, there is no reason to confine their application to any single realm of security. Instead, their greatest contribution to security may soon be in breaking down the silos of analysis. A ‘big data’ machine learning program that is plugged into many data streams within a facility (e.g., access control, human resources, cyber traffic, material accounting and maintenance schedules) could progressively establish more accurate concepts of the safe function baseline. This would then make the program better at identifying true anomalies. Refinement of such a system could help to bridge the safety-security sector divide that persists in the nuclear industry and enable security to keep pace with the complexity of increasingly complicated systems of systems.

Of course, AI systems bring with them not only the potential to enhance security but also the potential to undermine it. Notably, there exists a risk of over-reliance on and over-complication of these systems. If the introduction of an automated, all-watching sentinel is wrongly perceived to be a cure-all for security problems like insider threats, it may encourage a lack of vigilance or the deterioration of other human security functions. This might result in a net decline in security overall. If AI security analysis systems become too complex, adapting them to changing circumstances and validating their outputs could become extremely burdensome, to the extent that their use becomes counterproductive. Moreover, if such a system were relied upon for vital security functions and updates or validations of the system were done incorrectly it might feed bad signals to the human security personnel.

Additionally, as indicated in the Cyber Security section, even the most advanced AI tools are not likely to remain forever in the hands of defenders or legitimate organizations. Automated, AI powered cyberattacks appear to be close to reality and might drastically reduce the number of attackers and skill level needed to achieve certain types of cyber intrusions and certain levels of ultimate impact. These AI-driven advanced persistent threat capabilities might be particularly attractive to violent non-state actors who want to cause asymmetric cyber disruption but lack the number of skilled hackers that are presently needed to wage an ongoing, large-scale cyber-attack campaign. There is also the possibility that terrorists and other adversaries will employ AI to help them plan and conduct more efficient physical attacks on nuclear facilities, such as screening vast amounts of open source information to identify previously unrecognized vulnerabilities.

Perhaps even more worrying, however, is the prospect of AI system themselves being hacked. In the case that an AI system were used to monitor multiple streams of security data, infiltration of that system might serve as an ideal clearinghouse for information valuable to an attack plotter. Alternatively, if personnel with vital safety functions were to become overly reliant upon a virtual assistant program, a hacker might be able to inject false instructions so as to steer the employee unwittingly toward an act of sabotage or to facilitate a physical intrusion.

5.5 ENHANCED HUMAN PERFORMANCE

To date, the majority of cutting edge technologies for the enhancement of human performance have been directed at compensating for deficiencies in normal function that arise from illness, injury or genetic defect. These kinds of technologies would include developments like cochlear implants, prosthetic limbs, implanted electrical insulin pumps, blood vessel stents, or virtually any medical drug. In the coming decades, however, advances in chemistry, engineering and computing are likely to yield new technologies intended not to compensate for deficiencies, but to surpass the normal biological limitations of the human body. Like the rest of the technologies discussed here, human enhancements are likely to present opportunities for both facility defenders and attackers, though in this case the applications are unusually similar on the two sides.

While human workers in various parts of nuclear reactor facility operations might be made more capable with synthetic augmenting technologies, when thinking of enhancing security personnel, most enhancements are likely to come from military innovations. Given the relatively confined and brief nature of a nuclear facility attack event (when compared to a military campaign), it is not likely to be technologies that enhance endurance and survival that are adopted in the nuclear industry context. Rather, it is likely to be those technologies that heighten perception and cognition or boost physical strength. Among the most radical technologies with the potential to serve these ends are genetic engineering and neural, sensory or mechanical implants, though these are not likely to see implementation for security purposes for some time. What might arrive sooner, though, are a wide variety of focus, memory and emotion manipulating neuro-pharmaceuticals (nootropics), physical performance-enhancing drugs, and reality augmentation platforms.

With respect to the last of these, although present augmented reality (AR) systems make use of wearable equipment and would not strictly classify as human enhancement, the use of wearable systems might lead to the introduction of implanted AR systems in the near future. While current wearable systems allow for intuitive computer assisting of a multitude of tasks, implantation of AR systems will allow for new levels of effectiveness. This might enable new ways for facility attackers to covertly perform reconnaissance, interface with computer systems or communicate with collaborators while also enabling defenders to better do things like maintain and share operational awareness, target remote weapons or biometrically confirm identity. In the event that electronic enhancements or AR become common in facility defence, it should be remembered that this may introduce the potential for attackers to hack or scramble even the human element of the security response.

5.6 MODELLING AND SIMULATION

In the design and implementation of nuclear facility security systems there is thankfully little real world data to draw from in understanding what threats and vulnerabilities are of highest priority. There is also no option to wait for further data to become available (since this would imply that serious attacks have occurred). In light of this, modelling and simulation are vital in the design and testing of security measures. The creation of models and simulations that accurately reflect reality and appropriately prepare security forces, however, is neither a simple nor a settled practice.

Fundamentally, the degree to which simulation is helpful depends upon how accurately the underlying model(s) reflect real environments, agents and dynamics. There is thus always an incentive to make models more detailed. Yet every introduction of greater detail into a model runs some risk of misrepresenting reality. In modelling and simulation for nuclear facility security, on the one hand the complex environment and the need to account for very specific parameters requires a high level of detail. On the other hand, the ambiguous adversary and evolutions in both defensive and offensive technologies, in addition to a general desire to keep security or proprietary information secret, makes this difficult. This leaves modellers with the delicate task of needing to continually push their models to be as sophisticated and up-to-date as possible without straying beyond what can be supported with data or validated theory.

The prospects for advancing modelling and simulation in the future therefore rest mainly on improving the underlying data and theory. The defensive component of facility security models, as the known element, are more readily supported by empirical information—generally to the point that theoretical considerations are not necessary. For this reason, defensive aspects are usually modelled more accurately and in greater detail than threats.

There are, nonetheless, some areas where improvement is needed. The most basic of these is further standardization of how the input data is conceptualized, collected and implemented so as to allow for greater comparability between models (or simulation iterations) and more deliberate refinement of models (potentially aided by these inter-model or inter-simulation comparisons). The other way in which defender simulation can be improved is to incorporate more realistic conditions where the defender is faced with uncertain and ambiguous situations. While there may be abundant data available about the defender side, it is important to build simulations that do not give defenders unrealistic levels of awareness of adversary actions and also allow for defensive mistakes. Accounting for uncertainty and human error, particularly for actors under stress, is likely to remain among the most difficult defender characteristics to measure and model. This may become easier to model with improved threat assessment and easier to simulate with the introduction of more advanced augmented and virtual reality technologies.

More daunting than modelling the defender is the job of accurately modelling realistic adversaries. Because the adversary is necessarily hypothetical, the way it is represented in a model is based largely on theory and general terrorist attack patterns. Historically, the nuclear industry has attempted to get around this problem via the design-basis threat (DBT) concept. The intention of DBT is to prepare facility defences for any sort of adversary by presenting defenders with hypothetical adversaries that are at the very high end of potential attack capability.

The problem here is that preparing for a set level of adversary, even a very well-trained and well-equipped one, may not adequately prepare defenders for adversaries that also deploy unconventional weapons, innovative tactics or some combination thereof. For example, most current modsim in the nuclear facility context is focused on "neutralization of the threat" and currently has no capability to address more complex situations involving hostages, the use of non-lethal weapons, dealing with protestors etc. To examine these possibilities will require the use of horizon scanning and threat assessment techniques to keep ahead of developments in adversary tactics, techniques and procedures. It will also require further theoretical work to be sure that new technologies and creative tactics can be modelled without distortion.

Live simulations, including red teaming drills, can introduce a degree of authenticity and are often useful for testing existing levels of preparedness. However, these are sufficiently costly that they can be conducted only occasionally. In addition, these types of exercises can be prone to instilling a false sense of security if they fail to deviate from DBT or if they rely for their opposing forces exclusively on ex-military types who may not be preparing guards for an unconventional adversary. Expanding the range of simulations and developing new methods of selecting and simulating realistic adversary types and tactics can contribute greatly to security.

5.7 BIOMETRICS

The nuclear security industry was an early adopter of biometric screening at entry control points and continues to be a leading user.[76] The strict vetting procedures and access management of the nuclear sector in most countries is well suited to biometric entry controls. This is because the system is used to confirm a one-to-one match from a known database of those authorized to enter. Much of the work on improving biometric scanning is focused on moving away from more intrusive measures like finger and retina scanning and towards systems that work in less controlled environments (i.e. those that do not rely on bottlenecks like entry turnstiles) and with less active cooperation required on the part of those being screened. The leading technologies trying to accomplish this are facial recognition programs, although many such systems to date have been notoriously prone to error.[77] Considerable investment has been made, however, in improving the design and training of these systems in recent years.[78] Facial recognition systems are also now being paired with gait recognition systems to achieve a two factor verification process that can be run from the same camera images. Commercial applications such as banking and e-commerce are reportedly more advanced in many areas of biometrics than are security users.[79] It would certainly be feasible, however, for security contractors to license or otherwise adopt these improved technologies in the future.

The security advantages that advanced biometric screening can provide at nuclear facilities are certainly significant, but should also not be relied on blindly or to too great a degree. Biometrics remain vulnerable to some basic security defeats. First, an attacker could introduce new data into the records that monitoring systems reference, making the attacker a cleared individual.[80] An attacker with this sort of access might not only avert the suspicion of security personnel, but could also conceivably redirect suspicion toward legitimate personnel by removing them from the reference data. Second, many biometric screening measures have been followed closely by methods to fraudulently reproduce the necessary biometric identifiers.[81] Of course, biometric defences also do not prevent insiders with legitimate credentials from entering. Lastly, in the case of non-intrusive biometrics like facial recognition, these do not place the same amount of stress on those being actively screened, which could allow for non-technical detection of a problem.

5.8 CROSS-CUTTING ISSUES

5.8.1 CHALLENGES FOR REGULATION

The challenges regulators face in accounting for emerging technologies and the resulting changes in the threat posed to the nuclear industry generally relate to the difficulty of keeping pace with change while remaining tied to the broader currents in government and industry. Specifically, governments may pursue political goals to alternatively promote or restrict nuclear energy development that are entirely separate from scientific and technical progress or the threats and benefits that come from these developments. At the same time, some components of the nuclear industry might pursue novel, or even over-the-horizon technologies, while other elements seek to lock in their advantages. Each industry faction will pressure regulators accordingly. Navigating this environment requires regulators to be perceptive enough to see change coming (rather than just recognize much later that it has happened) and agile enough to react effectively to leverage technology where it favours the defence and guard against it when it favours the adversary. This is not a simple task, nor one that is likely to be the same between different countries. This is because this balanced regulatory approach must be done in a way that reflects the risk appetite of the state (which in liberal democracies is dependent in part on the risk tolerance of the public), while it must also be reasonable for industry to adhere to it.

Considering the continual acceleration of technological change, and the complexities of the threats and opportunities that emerge from these advances, it will become vital for both government and industry to institutionalize foresight activities. One way to do this is to utilize periodic or ongoing horizon scanning and net assessment efforts. In this regard, it must be recognized that, while regulators are not intelligence agencies, they will probably need the help of state security apparatuses to properly anticipate new threats.

Where the regulator has a greater role to play, and also more responsibility, is in developing and maintaining an agile posture. This means that regulators must be able to promote safety and security while accounting for rapid changes in the nature of threats and the readiness of industry to respond, particularly when these do not match up. With regard to technological changes specifically, it will be important for regulators to refrain from reflexively characterizing new technologies as problems, but to instead also recognize their potential benefits. In this way, regulators can empower rather than stifle novel solutions developed by industry. The rate at which technologies present new threats and opportunities simply will not accommodate the development and implementation of prescriptive regulatory solutions; instead regulators may have to become increasingly proactive in the facilitation and verification of outcome-based benchmarks.

At the same time, it will be difficult for regulators to give industry the latitude it needs to be innovative in responding to new security threats and coming up with customized industry solutions, while also ensuring that emerging threats are adequately and responsibly met. Of most concern is of course assuring that facility operators do not ignore technological threats that require redress and that they do not adopt technological defences that pose unacceptable new vulnerabilities or dangers to the public. There may, however, also be more nuanced decisions for regulators to make. Perhaps the most vital of these will be the assurance that security culture and the human element of security are not neglected amid operator enthusiasm for defensive “widgets.”

Technology and the Public

Regulators in democratic countries are indirectly beholden to represent public opinion regarding the degree of acceptable risk in the operation of nuclear power facilities, by way of elected governments. In the application of new regulation to mitigate threats posed by new technologies, however, there is also the potential for regulators to be hamstrung by popular opinion. In cases where a technology develops and is adopted by the public very quickly (UAS systems and ride sharing services being two recent examples), regulators may find themselves in a position where measures for the maintenance of security norms are difficult to formulate sufficiently rapidly. As a result, regulators might find themselves attempting to retroactively restrict a capability that the population has already embraced or even come to depend on. In these cases, it is possible that regulators "coming late to the party" might be stopped from enacting restrictions that are prudent ways to deal with a new technology because of fears of economic disruption or public backlash.

5.8.2 ETHICAL AND LEGAL CONSIDERATIONS

As regulators strive to keep up with technology, one of the greatest challenges is likely to be ensuring that legal frameworks can be updated quickly enough to enable the necessary defensive developments and the punishment of violators. Acknowledging that the law will often lag behind the emergence of the most disruptive technologies, there may be windows of opportunity for those intending to attack a facility to employ a new technology before effective countermeasures have been approved. In other cases, there may be some ambiguity about the legal limits of engagement in situations where new technologies are involved, which might help an attacker by delaying effective response to an attack. A clever attacker may indeed not try to tactically outmatch facility defenders, but rather to simply identify tactics that are legally the most difficult for defenders to promptly respond to. Currently such an opportunity could be said to exist with UAS technology, as it has been publically available for some time, but many of the most effective countermeasures are either yet to be legally approved or are prohibited under many circumstances. In the United States, regulations have only recently established drone "no-fly zones" around nuclear facilities while in Europe, even though over flights are technically illegal, this has not been matched with effective measures for attribution and punishment. Moreover, many of the regulations concerning over flights (whether of UAS or piloted aircraft) were designed with safety, as opposed to security, in mind and thus might require updating in many countries.

As alluded to in the section above, in addition to strictly adhering to the law, regulators and facility operators must also be aware of where the unwritten ethical boundaries associated with use of new technologies lie. These boundaries, if crossed, could inflame political or public opinion and bring additional problems for the facility operator or even the broader nuclear industry. The difficulty of this issue is illustrated virtually every time ostensibly non-violent activists breach facility security. These actors enter facilities in a way that would prompt a violent response from security forces if the intruders were observed to be armed or otherwise perceived to be threatening. As long as these actors appear not to have the intention to engage in violence or theft, however, the security response to their intrusion is subdued. This dynamic is nothing new to the nuclear sector, but nonetheless represents a paradigm that entails some risk – a risk that might, unnoticed, grow substantially as the result of technological development. It has long been possible for facility attackers to potentially buy themselves time and space to approach a facility by masquerading as someone more innocuous. On the one hand, the risk to the reputation of the industry if facility guards mistakenly wound or kill someone who is actually non-violent can make defenders accept a small chance that protestors could really be disguised attackers. Similarly, an overactive response to individuals acting "suspiciously" in areas adjacent to owner-controlled areas (where they might legally have the right to be) could prompt public or official backlash against even legitimate security measures. On the other hand, a lack of response could allow a threatening actor the opportunity to conduct reconnaissance and probe outer security measures unimpeded. New technologies could further complicate this dilemma – for instance where ROWS are installed – and security procedures and policies require careful reassessment (and potentially explicit protocol development) as technologies change.

6. SUMMARY AND RECOMMENDATIONS

Compared to terrorist attacks in general, and even to terrorist attacks against other critical infrastructure targets, attacks on nuclear facilities are exceedingly rare. Nonetheless, there have been several dozen plots, attacks or attempted attacks against such facilities, some of which may have been intended to result in mass casualties or mass disruption, making the threat non-trivial. Attacks on nuclear facilities can perhaps best be characterized as low probability, high-consequence events – where the introduction of new technologies might have a significant impact on the risk. This paper has therefore laid out recent and potential future trends in both terrorism and emerging technologies – and most importantly the intersection of these developments – as they relate to the nuclear industry. While the paper has discussed these topics in some detail, it is useful to highlight several points that warrant close attention, grouped into broad categories.

Developments in the terrorist threat:

- Most past nuclear terrorism activity has involved thefts from or attacks on nuclear facilities.
- Trends in attacks on nuclear facilities have in the past mirrored those in terrorism writ large, with a shift from attacks originating mostly from left-wing and ethno-nationalist adversaries to facility plots more recently coming from attackers predominantly motivated by more transcendent concerns.
- Although the recent “transcendent” terrorists have so far been less successful overall than the previous generation of terrorists when it comes to attacking nuclear facilities, their motivations make them more likely to seek to cause mass casualties in addition to disruption of operations.
- Actors claiming such transcendent motivations will continue to be the greatest terrorist threat, both in terms of their capability to engage in extreme violence and their ideological attraction to mass casualty attacks. As the most violent of such terrorist groups loses its territorial base in the Middle East, this will most likely result in fragmented successor groups whose overall capability will decrease but who might be more motivated to conduct spectacular attacks against very high-profile targets like nuclear facilities, either as acts of revenge or as bids for prestige within the now leaderless movement.
- The threat from these terrorists to facilities is likely to be greatest close to the areas where they are based, so the threat might hinge largely upon the degree to which nuclear energy takes root in the Middle East, North Africa, South Asia or Southeast Asia.
- In order for an emerging technology to constitute a terrorist threat, terrorists must first become aware of the technology’s potential utility, must then make a deliberate decision to pursue adoption of the technology, and – last but certainly not least – must successfully acquire and implement the technology in their tactical operations. As a result, only a relatively small proportion of terrorists pursue – and even fewer succeed in adopting – emerging technologies in the early years after their introduction.

Global shifts:

- Nuclear terrorism as a threat must be seen in the context of larger shifts in the global balance of power away from the United States and Western Europe and towards Asia. This is likely to force difficult adjustments in posture on the United States and its allies in terms of influencing global nuclear security.

- In this less stable geopolitical environment, there are likely to be more areas of conflict and instability, which could have far-reaching consequences for nuclear security. The security of facilities in zones of instability could be directly threatened by insurgents or warring parties, and instability and economic crisis can divert government attention and resources from radiological and nuclear security in general.
- Natural disasters, made more frequent by changes in global climate, could also put the security of nuclear facilities at risk and must be prepared for.
- The number of educated yet underemployed youth around the world could grow significantly, making instability and susceptibility to radicalization more likely among increasingly technically proficient populations.

Nuclear industry security:

- As the nuclear sector adapts to compete with inexpensive natural gas and maturing renewable energy technologies, security budgets will come under greater scrutiny at the same time as potential new threats and new facility designs will raise novel security challenges.
- The insider threat is a more important issue than ever and must receive even greater attention.
- Regulation must become more agile to allow for responsiveness to changes in the threat brought about by emerging technologies, since attackers can exploit the often lengthy periods of inertia where law lags behind technological development. Industry must be given the latitude to be innovative in responding to new security threats, while regulators need to ensure that emerging threats are adequately dealt with. Recommendations in this regard include:
    - Institutionalizing foresight mechanisms and structuring regulations to allow for rapid implementation of defensive measures while maintaining (and where necessary modifying) oversight and quality standards.
    - Ensuring that facility operators do not ignore technological threats that require attention or adopt technological defences that result in unacceptable new vulnerabilities.
    - There are ethical and public relations issues associated with the question of how facility security forces should react when confronted with ostensible protesters that could be attackers posing as well-meaning members of the public.

Emerging technologies:

Below characterizes and provides tentative recommendations for each of the specific emerging technologies discussed above.

Remotely Operated Weapons Systems (ROWS)

Character in Nuclear Context:

Defensive (with some potential for threat)

Recommendations:

Consider investing further in ROWS development as an adjunct to other countermeasures.

Caveat(s):

Do not become over-reliant on the technology and maintain redundancy in security; remain sensitive to vulnerabilities (especially cyber) and public perceptions.

Unmanned Aerial Systems (Drones)

Character in Nuclear Context:

Threat (with some potential for defence)

Recommendations:

Monitor developments and research various kinetic and non-kinetic detection and defeat options (including the use of UAS defensively to monitor)

Caveat(s):

Since defensive measures are nascent, make sure these are thoroughly tested and can be integrated into existing facility security before making investments.

Modelling and Simulation (modsim)

Character in Nuclear Context:

Defensive

Recommendations:

- Engage in modsim to help implement and improve security, including possible use of VR and AR.
- Standardize inputs for modsim across the industry
- Account for uncertainty and human / system error in models.
- Incorporate regular horizon scanning and threat assessment into modsim and other preparedness activities to counter deficiencies with DBT

Caveat(s):

Finding the correct balance between detail / granularity and real-world validation is difficult; DBT ignores adversary innovation; modelling the adversary is complex and not usually done robustly.

Biometrics

Character in Nuclear Context:

Defensive

Recommendations:

Continue to use and upgrade as new techniques mature

Caveat(s):

Remain mindful of fundamental weaknesses that can never be eliminated completely: insider threat and database manipulation.

Human Enhancement

Character in Nuclear Context:

Balanced (leaning toward defence due to accessibility and expense)

Recommendations:

- Possibly incorporate into defence, but only after a given technology has been tested thoroughly in another context or industry.
- When major new human enhancements become mainstream, assess the potential for these to change the DBT levels or significantly reduce the efficacy of specific security measures.

Caveat(s):

Monitor security forces for misuse; take into account unforeseen side effects for security operations; given the potential for hacking or malfunction, implanted or otherwise non-removable enhancements should be treated suspicion.

Cyber

Character in Nuclear Context: Threat

Recommendations:

- Core task: prioritize vulnerable nodes and focus attention on them
- Invest in “smart” detection and response capabilities
- Pay particular attention to cyber-physical nexus

Caveat(s):

It is difficult if not impossible to do 100% audits of vulnerabilities; cybersecurity must be integrated into overall security (especially human resources) to be effective (it cannot be standalone function).

AI

Character in Nuclear Context:

Defensive

Recommendations:

Employ for two main purposes:

- Blunting cyberattacks
- Combining silos of information (including human, system, and cyber) to look for patterns and anomalies that identify security threats and vulnerabilities in plant operations

Caveat(s):

Beware of over-reliance (can breed complacency and become critical failure node); defensive AI could be hacked to suit the ends of adversaries; adversaries might also use AI, especially for cyberattacks.

Emerging technologies will affect every aspect of society, including security. For the nuclear industry, this will present new sets of both threats and opportunities; some new technologies will be exploited by terrorists to challenge nuclear facility security and others can be used by defenders to bolster it. As is to be expected, there are many uncertainties related to the developmental trajectories of the technologies themselves and to the broader society in which they will mature. What is certain is that the nuclear industry cannot ignore these emerging technologies, for there are short windows in which to best prepare for their impacts, which will only grow over time.

ANNEX 1: NUCLEAR FACILITY INCIDENTS[82]

Date/Location	Description
January 3, 1961, United States SL-1 US Army Reactor at Idaho Falls	A reactor operator removed a control rod from the reactor, resulting in a power surge that broke the top of the reactor. This resulted in critical failure of the reactor vessel and irradiation of the building housing the reactor, killing all three occupants. Official reports classified the incident as a murder-suicide.
November 10, 1972, Oak Ridge, Tennessee Oak Ridge National Laboratory	Among other threats made by Melvin Cage, Louis Cale and Henry D. Jackson Jr. after highjacking a flight leaving Birmingham, Alabama, they threatened for a period to crash the DC-9 aircraft into the research reactor at Oak Ridge National Laboratory if they were not given $10 million. They circled the facility for an hour, forcing it to be shut down as a precaution. The hijackers eventually abandoned this ploy, eventually crash landing in Cuba.
March 3, 1973, Lima, Argentina Atucha Nuclear Power Plant	Fifteen armed men overwhelmed and disarmed a five-man security force at the site of the nearly finished Atucha-1 reactor. The attackers painted political slogans at the site before leaving, taking the overwhelmed guard's weapons with them. The attackers encountered and injured two other security personnel as they made their escape.
August 15, 1975, Brittany, France Brennilis Nuclear Power Plant	Breton separatists crossed the plant's artificial cooling lake by boat and cut through a fence in order to plant two bombs at the facility. The bombs detonated, damaging an air vent and a water inlet for the plant's cooling system. The reactor was temporarily shut down for inspection.

Date/Location	Description
January, 1977, Giessen, Germany Giessen Army Base	The Red Army Faction launched an attack on Giessen army base, with the ostensible objective of capturing or destroying nuclear weapons kept there. A diversionary bomb attack on fuel containers on the base was carried out by the RAF, but the intended impact was not achieved as the fuel did not ignite. A simultaneous assault on the armoury was repelled, with several RAF members killed in the process. The event received little publicity at the time and the presence of nuclear weapons on the base was initially denied.
October 10, 1977, Rainier, Oregon Trojan Nuclear Power Plant	A bomb exploded next to the plant's visitor centre (outside of the plant's gates) blowing out windows, causing injuries.
December 18, 1977, Lemoniz, Spain Lemoniz Nuclear Power Plant (Under construction)	Four ETA members attacked a guard station, one attacker was killed by security forces and the attack was repulsed. ETA later stated that they intended to blow up the reactor.
March 17,1978, Lemoniz, Spain Lemoniz Nuclear Power Plant (Under construction)	ETA members exploded a bomb in the steam generator room of the station (still under construction). The explosion killed two construction workers and injured 14 others, in addition to causing between 2 and 6 million dollars’ worth of damage.
February 19, 1979, Kaiseraugst, Switzerland Kaiseraugst Nuclear Power Plant	Bomb detonated, damaging the "Information Pavilion," causing $528,000 in damage.

Date/Location	Description
April 27, 1979, Surry, Virginia, USA Surry Nuclear Power Plant	Upset by loose safety procedures, Bill Kuykendall and James Merrill used Kuykendall's access card to enter the fuel building with five gallons of sodium hydroxide caustic soda. The two poured all five gallons over 64 new fuel assemblies, ultimately damaging 62 of them at an estimated cost of ~$810,000. Kuykendall said he chose to carry out a sabotage of this scale because it took an hour and twenty minutes, illustrating that a more malicious saboteur would have had plenty of time to do something far more dangerous. The two surrendered themselves when the damage was discovered.
June 13, 1979, Lemoniz, Spain Lemoniz Nuclear Power Plant (Under construction)	ETA guerrillas planted a bomb in the turbine room of the plant. Twenty-five minutes after a warning call, the bomb was detonated. One worker who did not evacuate was killed and a 5,000 litre tank of oil was ignited, causing moderate damage to turbine components.
November 11, 1979, Maliano, Spain Equipos Nucleares facility	Five ETA guerrillas planted explosives and kidnapped 10 guards. The bombs exploded at midnight that night causing $6,000,000 in damage to the main factory building. The guards were later released.
November 3, 1979, Däniken, Switzerland Gösgen Nuclear Power Plant	A bomb blast toppled a 330-foot weather control tower which fell on another part of the facility, causing ~$600,000 in damage. Plant function was reduced periodically but never totally interrupted. In a letter delivered to a TV station but addressing Swiss energy minister Willi Ritschard, the militant anti-nuclear group responsible stated that their intent was to prevent the official commissioning of the plant.

Date/Location	Description
Sometime in the 1970s, Kinshasa, Democratic Republic of the Congo Kinshasa Nuclear Research Center	Two 20% enriched uranium, fresh TRIGA II research reactor fuel rods were stolen from the Kinshasa Nuclear Research Center at the University of Kinshasa by unknown means and by an unknown party in the late 1970s. The rods may have been taken from the facility by members of the then-reigning regime in Zaire, perhaps under the direction of the dictator Mobutu Sese Seko himself. The stolen rods were of U.S. make and were provided under the Atoms for Peace program to Congo (then Zaire) in the 1970s for use in their newly built Triga II research reactor. One of the stolen rods was recovered in Rome in 1998 as part of an Italian police sting operation. Roman organized criminals with ties to the Catania and Magliana gangs provided the rod as a sample to business men and nuclear scientists they who they believed were representing a middle eastern buyer. The other rod was never recovered, nor were at least seven more the gangsters claimed to have had in their possession.
1981, Oswego, New York, USA Nine Mile Point Nuclear Power Plant	Deliberate closure of fuel oil filters led to the degradation of backup generators causing them not to start upon testing.
June 5, 1981, Shippingport Pennsylvania, USA Beaver Valley Nuclear Power Plant	Deliberate closure of a valve to the high head safety injection pumps compromised the emergency core cooling system. The padlock and chain meant to keep the valve in place were missing. There were no suspects and no arrests were made. In 1983, the NRC deemed it to be the most serious of 11 acts of suspected sabotage investigated since 1980.

Date/Location	Description
January 18, 1982, Creys-Malville, France Superphenix Fast Breeder Reactor	Five Russian-made anti-tank rockets were fired at the plant (still under construction) around midnight from a hill 600 yards away on the other side of the Rhone River, likely by Pacifist and Ecologist Committee member Chaïm Nissim. All five were thought to have been aimed at an opening in the reactor building. One passed though the opening striking a crane inside, one hit the outside of the main reactor building, one hit a metal crane outside, and the two others hit the wall of the steam generator building. The perpetrator escaped.
August, 1982, Salem, New Jersey, USA Salem Nuclear Power Plant	Manual isolation stop valves to the air start motors of the number 2C diesel generator were found closed. This would have prevented both automatic and manual startups had the generator been needed in an emergency. The act occurred during heightened security measures following a suspected act of sabotage a week earlier.
December 18, 1982, Cape Town, South Africa Koeberg Nuclear Power Station (Under construction)	uMkhonto weSizwe (MK) attacked the nearly completed Koeberg nuclear power plant in Cape Town, South Africa. Insider Rodney Wilkinson worked at the power plant for 18 months before stealing a set of plans and delivering them to the African National Congress in Zimbabwe. He then again gained employment at the Koeberg plant for piping work after being prompted to do so by ANC. After practice penetrations of the plant's security, Wilkinson placed four limpet mines at the power station—two on reactor heads and two under the control rooms. Wilkinson was responsible for smuggling the mines in and setting them on timers such that they would detonate when the facility was relatively empty and after he had escaped. The opening of the plant was delayed by 18 months as a result.

Date/Location	Description
December 4, 1983, Schwabisch Gmund, West Germany Hardt Military Barracks	Four activists from the "Plowshare 8" branch of the Plowshares anti-nuclear group cut through a fence shortly after 8 AM and damaged a tractor of the kind used to transport Pershing 2 nuclear armed missiles using crowbars and other tools. They were on site for 15 minutes before being surrounded by guards. The site of the breach was ultimately a 30 minute drive from the nearest missile site.
November 12, 1984, Higginsville, Missouri, USA Minuteman ICBM silo	Four catholic peace activists, Rev. Carl Kabat, Rev. Paul Kabat, Helen Woodson, and Larry Cloud-Morgan from the Silo Pruning Hooks organization entered the grounds of a Minuteman ICBM silo and did over $10,000 in damage to the facility with a jackhammer and other tools. All four were arrested and convicted of conspiring to impede national defense.
June, 1985, Wintersburg, Arizona, USA Palo Verde Nuclear Power Plant	Four sets of valves were tampered with, causing a sharp drop in cooling system water pressure.
June 4, 1985, Bataan, Philippines Bataan Nuclear Power Plant (Under construction)	Twenty-six bombs were discovered placed around the facility.
June 28, 1985, Bataan, Philippines Bataan Nuclear Power Plant (Under construction)	Dynamite charges were used to damage 13 transmission towers connected to the nearly completed plant.

Date/Location	Description
May 14, 1986, Wintersburg, Arizona, USA Palo Verde Nuclear Power Plant	Power transmission lines leading away from the plant were cut.
November 28, 1987, Livermore, California, USA Sandia National Laboratories	A bomb exploded at 1:30 AM under a car in the parking lot, destroying that car and another. The explosion also shattered two windows of a nearby weapons lab.
February, 1990, Azerbaijan Soviet Weapons Depot	Azerbaijani rebels attacked a Soviet weapons depot housing nuclear weapons. The attack was unsuccessful and Soviet troops secured the base.
1991–1992, Glazov, Russia Chepetsky Metallurgical Plant	At least 12 people, including facility employees and security personnel, stole a sizeable amount of uranium (indicated to be natural and depleted uranium) by diverting 4% of the "allowed inventory loss" each month for several months. They would smuggle it elsewhere after accumulating a sizable amount. The Russian FSB seized at least some (possibly all) of the stolen material. Later inventory checks revealed that a total of 300 kg of uranium was missing from the facility.
May–Sep, 1992, Podolsk, Russia Luch Scientific Production Association*	On over twenty occasions, over the course of five months, Leonid Smirnov, a chemical engineer at the facility, walked out with 50–70 g of 90% HEU at a time, carried in a jar. He accumulated ~1.5 kg at his apartment (on the balcony) before being arrested prior to attempting to transport it to Moscow. He said he was inspired by a newspaper article which told of the money to be made on the nuclear black market. He was sentenced to probation.

Date/Location	Description
1992, Visaginas, Lithuania Ignalina Nuclear Power Plant	A 280 kg LEU fuel assembly containing 100 kg of LEU was tied to the bottom of a duty bus and successfully smuggled out of the facility.
1992, Udmurtia, Russia Unspecified Facility	A man arrested smuggling 2.5 kg of uranium into Poland admitted having already smuggled 3 kg and to being part of a larger group that was planning to steal a total of 100 kg of uranium-238 from a "plant" in Udmurtia, Russia and smuggle it into Poland.
January, 1992, Visaginas, Lithuania Ignalina Nuclear Power Plant	Insider technician and software programmer, Oleg Savchuck, was arrested attempting to introduce a virus into the Ignalina Power Plant's computer system. The plant also experienced a breakdown in the first reactor's cooling system, but the two incidents' connection has not been confirmed.
1993, Kola Peninsula, Russia Andreeva Guba Technical Base	At least three insiders (two servicemen and at least one security guard) conspired on at least one occasion to steal 1.8 kg (in one report 3.6 kg) of ~35% HEU from two naval reactor fuel assemblies. Guards manning the alarm post were said to have cooperated with the theft. The material would later be recovered and the perpetrators sentenced to 4-5 year prison terms. Those convicted claimed they were acting under orders from two officers. The officers, however, denied the claims and were found not guilty.
1993, Moscow Oblast, Russia Elektrostal Plant	Reports surfaced that guards at the facility would turn off the security at the facility for short periods in exchange for 1,000 rubles. Another report from the same time period indicated that 3.05 kg HEU had been stolen from the facility. Material that may have been the material missing from this facility was discovered in St. Petersburg in June 1994.

Date/Location	Description
February 8, 1993, Londonderry Township, Pennsylvania, USA Three Mile Island Nuclear Power Plant*	Having recently been released from a mental ward, Pierce Nye drove his station wagon through an open outer gate to the facility during a changing of the guard around 7 AM. He then crashed through another inner gate before ultimately crashing into a roll-up door to the plant's turbine building. From this point he proceeded on foot, spending four hours in the plant before being found hiding under a grate on the first floor of the turbine building. He was not armed and never accessed areas of the plant considered vital.
April 4, 1993, Moscow, Russia Orel Branch, Moscow Instrumentation Research and Development Institute[83]	Employees of the Orel branch of the Moscow Instrumentation Research and Development Institute were arrested while attempted to sell 75 grams of plutonium that they had smuggled out of the plant.
November, 1993, Severomorsk, Russia Severomorsk Naval Yard	A Russian naval officer and at least two accomplices stole 4 kg of enriched uranium (20% U-235) from a poorly guarded part of the base. He was later caught but his sentence was suspended in return for him giving up his two accomplices who were then sentenced to three years in a labor camp.
November 1993, Chelyabinsk, Russia Zlatoust-36 Instrument Plant	Two employees of the plant reportedly stole two nuclear warheads from a warhead assembly facility. The weapons were recovered in a nearby residential garage and the two employees arrested shortly thereafter.

Date/Location	Description
November 27, 1993, Murmansk, Russia Sevmorput Shipyard	Retired navy captain Alexei Tikhomirov was briefed on the scant security at the facility by his brother, who was the civilian chief of refueling there. Tikhomirov slipped through an unprotected gate and then through a hole in the fence around the fuel storage facility. He then pried open a padlocked door to the fuel storage building. Inside he located containers of fresh submarine fuel assemblies and took three from a VM-4-AM reactor core. He put the 4.5 kg of uranium (~20% U-235) into a bag and retraced his steps to escape. The theft was first identified because he left the door open. Tikhomirov was caught and the material recovered six months later after he had asked a fellow officer for help in selling the material. He was seeking $50,000 in exchange for the uranium.
1994, Moscow Oblast, Russia Elektrostal Plant	An employee smuggled almost 3 kg of 90% enriched uranium out of the Electrostal Machine-Building Plant (major producer of Russia's naval and research reactor fuel) hidden in his protective gloves.
March, 1994, Barnaul, Siberia, Russia SS-25 ICBM site	A soldier opened fire with a sub-machine gun, killing his commander and two other soldiers at a Russian SS-25 mobile ICBM site. Other soldiers would not return fire for fear of hitting the SS-25. The attacking soldier took refuge in an armored vehicle but was persuaded to surrender after three hours.
April 4, 1994, Moscow Oblast, Russia Elektrostal Plant	Convinced by his cousin Rogov, an employee named Lugachev stole 1.76 kg of uranium from the plant. The buyer they found, a man named Kharif, turned out to be an FSB agent.

Date/Location	Description
August, 20, 1994, Nizhny Novgorod Oblast, Russia Sarov (formerly Arzamas-16)	Three teenagers stole 9.5 kg of natural uranium from the closed city of Sarov, a centre for Russian nuclear research. Apparently they hoped to sell the material for money to buy video equipment.
1995, Moscow Oblast, Russia Elektrostal Plant	An employee smuggled 1.7 kg of 21% enriched uranium out of the facility in a shopping bag full of apples. The theft was not detected in progress due to the portal monitors not working at the time.
December 4, 1995, Blaye, France Blayais Nuclear Power Plant	Saboteurs put salt into the cooling contour of one of the reactors intending to cause a meltdown.
January, 1996, Sovietskaya Gavan, Russia Sovietskaya Gavan Naval Base	Three workers reportedly stole fuel rods containing at least 7 kg of HEU.
January 9, 1996, Kizlyar, Russia Russian Military Airfield	Chechen fighters unsuccessfully attacked a Russian military airfield likely housing nuclear weapons.
September 25, 1996, Oak Ridge, Tennessee, USA Y-12 National Security Complex	Charles Stevens Roddy, a janitor at the Y-12 nuclear facility, attempted to steal a device consisting partly of depleted uranium from a waste barrel that was marked as "classified secret" and "radioactive material." Roddy was arrested after setting off the radiation detection system at the plant's employee exit. He claimed he wanted to make the piece into a paperweight. After an investigation, stolen computers from the Y-12 Federal Credit Union were uncovered at Roddy's house.

Date/Location	Description
March, 1997, Kursk Oblast, Russia Kursk Nuclear Power Plant	Five unarmed men broke into the Kursk Nuclear Power Plant. The group were initially thought to be associated with an environmental group, but the likely cause for intrusion appears to have been strictly criminal. The five men were able to reach the plant generator, intending to disable the reactor and seize the control room, but lacked any capability to accomplish this.
December 27, 1997, Crystal River, Florida, USA Crystal River Nuclear Power Plant	Donald Beauregard was planning to lead a strike team in an explosives attack on the Crystal River nuclear power plant in St. Petersburg, Florida. One account states the reactor was the target while another stated only that the plan was to knock out power to the facility, forcing it to shut down. An informant tipped off police, allowing the plan to be interdicted before execution. Beauregard led the Southeastern States Alliance, an anti-government militia.
January 11, 2000, Tokaimura, Japan JCO Uranium Processing Plant	Tatsufumi Oshiba of Annaka was arrested after planting a homemade bomb near the uranium processing plant belonging to JCO Co. in Tokaimura, Japan. The bomb did not go off because the timer on the bomb had not been started. Oshiba confessed to further plans to bomb the JCO Company's uranium processing plant in Tokaimura, which was the victim of a 1999 nuclear accident. He stated he was motivated by anger over the previous incident.

Date/Location	Description
March, 2000, Sydney, Australia Lucas Heights Nuclear Reactor	Two Afghan men were arrested in New Zealand in March 2000 on charges of fraudulently using documents for purposes of immigration. They were suspected of having planned an attack on the Lucas Heights Nuclear Reactor outside of Sydney, Australia. Australian police discovered the forged documents plot while investigating a criminal organization involved in money laundering and immigration crimes. The men were reported to have had some connection to Osama Bin Laden and to have been in possession of a map of Sydney on which a reactor facility and routes to it had been highlighted.
March 6, 2000, Rostov-na-Donu, Russia Nuclear Research Institute	A remotely detonated bomb exploded at the nuclear research facility in Rostov-na-Donu, injuring two. Though the event was initially rumored to have inflicted high casualties and caused a release of radiation, those reports were false. The bombing is thought to have been the result of mafia infighting. Russian authorities also stated that at the time of the attack there was no longer nuclear research being conducted at the facility.
September 5, 2000, Bern, Switzerland Mühleberg Nuclear Power Plant	An anti-nuclear activist landed a motorized parafoil on the roof of the reactor building.
September 13, 2001, Kleine Brogel, Belgium Kleine Brogel Air Base	Nizar Trabelis admitted to having plotted to drive a car bomb into the Kleine Brogel air base, where US nuclear weapons are reportedly housed. Trabelis apparently intended to target the mess hall, however, as he sought to kill American service members. Tunisian Trabelis was reportedly among a group of Islamic radicals plotting attacks for Al-Qaeda and the Taliban.

Date/Location	Description
October 6, 2001, Zehlendorf, Germany Hahn Meitner Institute for Nuclear Research	Members of the al-Tawhid group hired two aircraft to perform surveillance for a potential attack on the Hahn Meitner Institute for Nuclear Research (HMI) in Zehlendorf, Germany. Thirteen individuals were apprehended as a result.
2002, Cape Town, South Africa Koeberg Nuclear Power Station	Three men and three women approached on inflatable dinghies and scaled a wall to infiltrate the Koeberg Nuclear Power Plant and hang a large sign reading "Nukes Out Of Africa."
January, 2002, Cumbria, United Kingdom Sellafield Nuclear Complex	British law enforcement discovered a plot by the Real IRA to steal plutonium from the Sellafield Nuclear Complex. The group members had reportedly already unsuccessfully traveled to Serbia and Croatia in attempts to buy the material. No arrests were made.
October 14, 2002, Suffolk, England Sizewell B Nuclear Power Plant	150 activists entered the site unopposed through the main gate and through the perimeter fence. They were inside the security perimeter for 25 minutes before being confronted by two security guards. The activists stated their intent was to protest government plans to build new nuclear power stations.

Date/Location	Description
May, 2003, Normandy, France Cap de la Hague Reprocessing Plant	Arrests of several members of the Salafiyya Jihadiyya group following the 2003 bombings in Casablanca, Morocco led to the uncovering of a suicide bomb plot targeting a French nuclear power plant, as well as plans to attack several trucks carrying powdered plutonium from a reprocessing plant in Cap de la Hague to sites in Belgium, Holland, and Germany. Pierre Robert, who received training while in Al-Qaeda camps in Afghanistan, divulged these plans, though his suspected role in the plots is limited. Other key figures are Abdelaziz Benlaich, the would-be suicide bomber, and Abdelkrim Mejati, who was behind the Moroccan attacks and may have been involved with the nuclear terrorist plots.
November, 2003 Sydney, Australia Lucas Heights Nuclear Reactor	Two Pakistani born Australians, Faheem Khalid Lodhi and Izhar ul-Haque, where charged in 2004 with having worked with French national Al-Qaeda associate Willie Virgile Brigitte to plot a bombing attack on the Lucas Heights reactor in November of the year before. Brigitte was not arrested but deported to France.
May 15, 2008, Dera Ghazi Khan, Punjab, Pakistan Dera Ghazi Khan Conversion Facility[84]	Baloch separatist fighters opened fire on the facility with mortars. Though no damage is said to have been done to any nuclear facilities on site, service buildings and a cafeteria were reportedly struck. Additionally, the munitions set fire to a section of woods near the facility which took 10 hours to extinguish. One report indicated that it was specifically a waste site, associated with the Baghalchur Uranium Mine, that was targeted.

Date/Location	Description
November 8, 2007, Pelindaba, South Africa Pelindaba Nuclear Facility	On the night of Nov. 8th, 2007, the Pelindaba Nuclear Facility, 18 miles west of Pretoria, was attacked by eight men, split into two four-man teams, who simultaneously attacked secluded points of the outer security perimeter. One of the teams cut an outer fence and exchanged gunfire with a facility guard but was held off at the outer perimeter until they eventually fled. Meanwhile, the other team raised a portion of the electrified outer fence with a plastic clip enough for one man to crawl under. This man proceeded to disable the alarm for that portion of the fence, cut the communications cable to the security office, and finally disable the electrification, allowing the remaining three members of his team to enter. These events were caught on a security camera but no alarms were raised. Once inside, the intruders disabled the security cameras, an event which also went unaddressed by facility security. This group then made their way directly to the emergency control centre three-fourths of a mile from their initial breach point. They are reported to have then taken a ladder from a garage housing fire engines and used it to enter the emergency control building through a window. Inside, the chief of the emergency control centre was able to call for security before being assaulted and shot in the chest. Security took 24 minutes to respond (21 minutes longer than expected) and found the wounded chief of security. These four intruders spent 45 minutes within the facility's security perimeter without encountering security forces and escaped though the same opening in the fence they had created to enter. All eight escaped but three men who remain unidentified were later arrested in connection to the attack.

Date/Location	Description
2010, Kleine Brogel, Belgium Kleine Brogel Air Base	A group of peace activists climbed the fences at the Kleine Brogel Air Base and placed banners on shelters which have been housing US nuclear weapons. The Belgian Ministry of Defense claimed that the activists were not “anywhere near a sensitive area”, and instead the bunker in question was empty.
February 15, 2011, Cofrentes, Spain Cofrentes Nuclear Power Plant	As many as 20 Greenpeace activists scaled a cooling tower at the Cofrentes Nuclear power plant, hanging banners to protest the renewal of the nuclear plant’s license. Spanish authorities indicated that vital components of the plant were never at risk.
December 5, 2011, Nogent-sur-Seine, France Nogent Nuclear Power Plant	Nine Greenpeace activists bypassed outer security at the Nogent-sur-Seine nuclear power plant, where they were immediately detected and followed by security on site. The group scaled a reactor building to unfurl banners renouncing the safety of nuclear power. Seven of the nine intruders were quickly arrested, while the other two were later found and arrested after hiding on site.
April 28, 2012, Pelindaba, South Africa Pelindaba Nuclear Facility	A failed breach of the Pelindaba nuclear facility wherein the would-be intruders failed to defeat any security systems. No arrests were made.
May 2, 2012, Bugey, France Bugey Nuclear Power Plant	A Greenpeace activist operating a powered paraglider dropped a smoke flare onto the roof of a building at the Bugey nuclear power plant before landing and being arrested by on site police authorities. A Greenpeace spokesperson acknowledged that the incident was intended to demonstrate the vulnerability of French facilities to aerial attacks.

Date/Location	Description
July 28, 2012, Oak Ridge, Tennessee, USA Y-12 National Security Complex	An 82-year-old nun and two fellow senior Plowshares activists breached the Y-12 National Security Complex. The three intruders entered through a series of fences with bolt-cutters and proceeded to vandalize the facility that houses HEU. Degraded security culture and defective security technology allowed the trespassers to remain on site undisturbed for two hours.
August 16, 2012, Kamra, Pakistan Minhas Air Force Base*	TTP affiliated militants attacked the Minhas Air Force Base, which allegedly houses Pakistani nuclear warheads. Approximately nine militants were dressed in official air force uniforms and armed with automatic weapons, RPGs, and suicide vests. Several attackers remained outside of the base, firing RPGs, while the remaining forces scaled the wall and engaged the base security for five hours. They never gained access to nuclear materials.
October 9, 2012, Varberg, Sweden Ringhals Nuclear Power Plant	Twenty Greenpeace activists breached the perimeter and rode bicycles around the facility grounds. Police arrived after 40 minutes, with 16 people arrested.
October 9, 2012, Forsmark, Sweden Forsmark Nuclear Power Plant	Fifty Greenpeace activists climbed over perimeter fences to gain access to the facility. Police arrived after 15 minutes and arrested all 50 intruders.
April 21, 2013, Rhea County, Tennessee Watts Bar Nuclear Power Plant	A man approached the Tennessee Valley Authority Watts Bar Nuclear Plant on a boat and proceeded to enter a restricted area housing a nuclear reactor. Here he fired several shots at a security guard with a handgun before fleeing, again by boat.

Date/Location	Description
March 5, 2014, Oskarshamn, Sweden Oskarshamn Nuclear Power Plant	About 20 Greenpeace activists used ladders to scale three perimeter fences and gain access to the facility. Six then climbed to the roof of the reactor building and unfurled a banner.
March 18, 2014, Fessenheim, France Fessenheim Nuclear Power Plant	Approximately 60 Greenpeace activists from 14 countries entered the Fessenheim nuclear power plant grounds, hanging a banner on a reactor reading "Stop Risking Europe." Helicopter borne law enforcement arrested the activists who had climbed the reactor, with officials assuring the public that no impact was made on the plant's operation.
July 9, 2014, Dimona, Israel Negev Nuclear Research Center	Hamas' militant Qassam Brigades fired at least three rockets towards the Negev Nuclear Research Facility south-east of Dimona. One rocket was intercepted by IDF's Iron Dome, and the other two landed in open areas. These rockets were but three of the 74 fired into Israel that day.
August 5, 2014, Doel, Belgium Doel Nuclear Power Plant	An apparent sabotage released oil to an underground storage tank, causing the overheating and shutdown of the Doel 4 turbine.
September 10, 2014 (first occurrence), France and Belgium Various nuclear power plants	Over the course of September and October 2014, 13 French nuclear power facilities were overflown on at least 15 separate occasions by remotely operated drone aircraft. Five sites were overflown on October 31st alone. Since then there has been at least one overflight of the same profile at the Doel Nuclear Power Plant in Belgium. The party or parties responsible have not been apprehended or identified and their exploits may be ongoing as of this writing.

Date/Location	Description
October 8, 2014, Tamil Nadu, *India Madras Nuclear Power Plant*[85]	A head constable with the Central Industrial Security Force opened fire with a service weapon at the plant, killing three and injuring two before surrendering.
April 4, 2016, Bavaria, Germany Gundremmingen Nuclear Power Plant[86]	Viruses were found at Gundremmingen's B unit computer systems, which are associated with equipment for moving nuclear fuel, and on 18 removable data drives, mostly USB keys, in office computers maintained separately from the plant's operating systems. The virus W32.Ramnit is designed to steal files from computers and give an attacker remote control over a system when connected to the internet. The virus Conflicker spreads through networks and by copying itself onto data drives. It is unclear whether the plant was infected intentionally or coincidentally.

REFERENCES

[1] David C. Rapoport. “The Four Waves of Modern Terrorism.” in Attacking Terrorism: Elements of a Grand Strategy. ed. Audrey Kurth Cronin and James M. Ludes. (Washington D.C.: Georgetown University Press, 2004), 46–47.

[2] In the original exposition of the “waves” conceptualization of terrorism trends, the author points out that each wave has typically lasted no longer than a human generation, indicating that each wave dies along with the last of those who initially championed the philosophy. Following from this, the author speculates that the present religious wave may give way to the next milieu at some point in the 2020s. Ibid.

[3] The features which rise to characterize each wave of terrorism are not necessarily only taken up by actors as earnest motives but may also rise, at least in part, for their being effective “mechanisms for moral disengagement” or enhancing the stylishness of violent activities. Albert Bandura. “Mechanisms of moral disengagement,” in Origins of Terrorism: Psychologies, Ideologies, Theologies, States of Mind. ed. Walter Reich (Cambridge: Woodrow Wilson International Center for Scholars and Cambridge University Press, 1990).; Martha Crenshaw. “The Debate over “New” vs. “Old Terrorism.” American Political Science Association, Chicago. August 30–September 2, 2007. 14.

[4] Martha Crenshaw. “The Debate over “New” vs. “Old Terrorism.” American Political Science Association, Chicago. August 30–September 2, 2007. 31.

[5] National Consortium for the Study of Terrorism and Responses to Terrorism (START). 2016. Global Terrorism Database. Retrieved from https://www.start.umd.edu/gtd. Data is presently incomplete for the year 1993.

[6] James Halverson and Gary Ackerman. Radiological/Nuclear (RN) Terrorism: Global Assessment of Threat Intention Drivers. College Park, MD: START, 2015.

[7] Gary A. Ackerman and Markus K. Binder. 2017. “Pick Your POICN: Introducing the Profiles of Incidents involving CBRN and Non-State Actors (POICN) Database.” International Studies Association Annual Meeting in Baltimore, 2017.

[8] The remainder of violent incidents are either of unknown motivation or entail actors who had a criminal profit motive. Eight of the 35 plots featuring violent intentions did not progress beyond plotting stages.

[9] See Nuclear Facility Incident Annex for examples.

[10] Gary Ackerman and James Halverson. “Attacking Nuclear Facilities: Hype or Genuine Threat?.” in Nuclear Terrorism: Countering the Threat. ed. Brecht Volders and Tom Sauer. (London: Routledge, 2016).

[11] Among the cases featured in the Nuclear Facility Incident Annex, cases like the 2008 mortar attack in Pakistan and the 2014 rocket attack in Israel seem to suggest at least an attitude of indifference to the potential of inducing a radiological hazard on the part of the attacker.

[12] Data from Critical Infrastructure Terrorist Incident Catalog (CrITIC) which was included 5689 cases updated through 2005. 43% of incidents were of unknown ideological motivation and much smaller numbers were classified as state-sponsored (1%), criminal (1%), or other (6%). Only three cases are classified as right-wing. See “Assessing Terrorist Motivations for Attacking Critical Infrastructure.” 2006. Weapons of Mass Destruction Terrorism Research Program, Center for Nonproliferation Studies, Monterey, CA.

[13] Halverson, James and Daniel Smith. 2017. “Nuclear Infrastructure as a Target: Identifying the Contextual and Ideological Factors Underlying Attacks against Nuclear Facilities.” Annual Meeting of the International Studies Association, Baltimore.

[14] Ackerman, Gary, et. al. 2006. “The Jericho Option: Al-Qaeda and Attacks on Critical Infrastructure.” June 8. Center for Terrorism and Intelligence Studies, San Jose, CA. p. 97.

[15] Ackerman, Gary, et. al. 2006. “The Jericho Option: Al-Qaeda and Attacks on Critical Infrastructure.” June 8. Center for Terrorism and Intelligence Studies, San Jose, CA.

[16] Ackerman, Gary A., Jeffrey M. Bale, and Kevin S. Moran. 2007. “Assessing the Threat to Critical Infrastructure.” In Weapons of Mass Destruction and Terrorism, edited by James J.F. Forest and Russell D. Howard, 305-326. New York: McGraw-Hill Education.

[17] Miller, Erin. 2016. “Terrorist Attacks Targeting Critical Infrastructure in the United States, 1970-2015.” Report to the Office of Intelligence and Analysis, U.S. Department of Homeland Security, June. START, College Park, MD. https://www.start.umd.edu/pubs/DHS_I%26A_GTD_Targeting%20Critical%20Infrastructure%20in%20the%20US_June2016.pdf

[18] On the other hand, if jihadist actors have considered the targeting of nuclear facilities in the way that Al-Qaeda approached transportation—as a means by which critical infrastructure targeting can maximize casualties—then the world would certainly be dealing with a new sort of terrorist threat to nuclear facilities; one that aims to induce a release of radiation as a matter of course.

[19] Miller, Erin. 2016. "Terrorist Attacks Targeting Critical Infrastructure in the United States, 1970-2015." Report to the Office of Intelligence and Analysis, U.S. Department of Homeland Security, June. START, College Park, MD. https://www.start.umd.edu/pubs/DHS_I%26A_GTD_Targeting%20Critical%20Infrastructure%20in%20the%20US_June2016.pdf

[20] The coding variables in the Global Terrorism Database do not always correspond directly with the CI sectors as identified by the Department of Homeland Security, so in some cases it is up to the researchers' discretion as to which target variables constitute CI and which do not. For some, there is a 1:1 correlation. For instance the GTD target subtypes Ambulance, Fire Fighter/Truck, Police Building, Police Checkpoint, Police Patrol, and Police Security Forces fit neatly into the Emergency Services Sector. In cases such as Chemical Sector or Nuclear Reactors, Materials, and Waste Sector, the authors relied on keyword searches within the GTD to tease out relevant cases which may lead to some inadvertent oversight due to coding irregularities in the dataset itself. As much as feasible, the authors attempted to replicate Miller's inclusion criteria modified by feedback received after publication of the above-cited 2016 article and adapted for differing definitions of CI in the authors' previous work (Authors' correspondence with Erin Miller, April 4).

[21] The GTD underreports attacks on nuclear facilities due in part to inclusion criteria. A more thorough accounting of attacks on nuclear facilities is available from START's Nuclear Facilities Attack Database (NuFAD) which currently lists 80 incidents. An updated and expanded version of NuFAD compiled by the authors of this report is due out in 2018. For a description and analysis of NuFAD as it currently exists, see Ackerman, Gary A. and James Halverson. 2016. "Attacking Nuclear Facilities: Hype or Genuine Threat?" in Brecht Volders, Tom Sauer (eds.) Nuclear Terrorism: Countering the Threat. New York: Routledge.

[22] Warrick, Joby. 2017. "Use of Weaponized Drones by ISIS Spurs Terrorism Fears." Washington Post, February 21. https://www.washingtonpost.com/world/national-security/use-of-weaponized-drones-by-isis-spurs-terrorismfears/2017/02/21/9d83d51e-f382-11e6-8d72-263470bf0401_story.html

[23] Ismay, John, Thomas Gibbons-Neff, and C.J. Chivers. 201. "How ISIS Produced Its Cruel Arsenal on an Industrial Scale." The New York Times, December 11. https://www.nytimes.com/2017/12/10/world/middleeast/isis-bombs.html?emc=edit_nn_20171211&nl=morningbriefing&nlid=76797135&te=1. "Standardisation and Quality Control in Islamic State's Military Production" 2016. Conflict Armament Research. December 1. http://www.conflictarm.com/publications/

[24] Strack, Columb. 2017. "The Evolution of the Islamic State's Chemical Weapons Efforts." CTC Sentinel. 10:9. October. https://ctc.usma.edu/the-evolution-of-the-islamic-states-chemical-weapons-efforts/

[25] Gallagher, Sean. 2016. "As US Drops 'Cyber Bombs,' ISIS Retools its Own Cyber Army." Ars Technica, May 28. https://arstechnica.com/information-technology/2016/04/as-us-drops-cyber-bombs-isis-retools-its-own-cyber-army/

[26] Ackerman, Gary and James Halverson. 2016. "Research Support for Net Assessments: Insight Compendium." November 8. START, College Park, MD.

[27] Halverson, James and Daniel Smith. 2017. "Nuclear Infrastructure as a Target: Identifying the Contextual and Ideological Factors Underlying Attacks Against Nuclear Facilities." Paper presented at the ISA Annual Meeting, Baltimore, February 22-25, 2017.

[28] O'Brien, Fergal. 2018. "Trump's Trade War and the $470 Billion Hit to the Global Economy." Bloomberg, March 12. https://www.bloomberg.com/news/articles/2018-03-12/trump-s-trade-war-and-the-470-billion-hit-to-the-global-economy

[29] U.S. National Intelligence Council. 2017. "Global Trends: Paradox of Progress." Office of the Director of National Intelligence. https://www.dni.gov/files/documents/nic/GT-Full-Report.pdf

[30] Gordon, Michael. 2018. "Forecasting Instability: The Case of the Arab Spring and the Limitations of Socioeconomic Data." Middle East Program, February 8. Wilson Center, Washington, DC. https://www.wilsoncenter.org/article/forecasting-instability-the-case-the-arab-spring-and-the-limitations-socioeconomic-data%20

[31] Chief among these groups are the likes of Chechen separatists in Russia, Baloch separatists in Pakistan, and the Houthi rebels in Yemen.

[32] Zolli, Corri. 2016. “Lone Wolf or Low-tech Terrorism? Emergent Patterns of Global Terrorism in Recent French and European Attacks.” Lawfare, August 17. https://www.lawfareblog.com/lone-wolf-or-low-tech-terrorism-emergent-patterns-global-terrorism-recent-french-and-european

[33] Ackerman, Gary, et al. 2018. “Horizon Scan of Non-State Actuated RN Threats and Defense Opportunities: Insights Compendium.” Final Report to NNSA. START, College Park, MD.

[34] Giroux, Jennifer and Peter Burgherr. 2012. “Canvassing the Targeting of Energy Infrastructure: The Energy Infrastructure Attack Database.” Journal of Energy Security, July. http://www.ensec.org/index.php?option=com_content&view=article&id=379:canvassing-the-targeting-of-energy-infrastructure-the-energy-infrastructure-attack-database&catid=128:issue-content&Itemid=402

[35] Ross, Michael L. 2008. “Blood Barrels: Why Oil Wealth Fuels Conflict.” Foreign Affairs. 87:2-8.

[36] Mills, Robin. 2016. “Risky Routes: Energy Transit in the Middle East.” Brookings Doha Center Analysis Paper Number 17, April. Brookings Institute, Doha, Qatar. https://www.brookings.edu/wp-content/uploads/2016/07/en-energy-transit-security-mills-2.pdf

[37] Mouchantaf, Chrine. 2018. “How a Disputed Oil and Gas Field Could Be The Last Straw for Israel and Lebanon.” Defense News, February 8. https://www.defensenews.com/global/mideast-africa/2018/02/08/how-a-disputed-oil-and-gas-field-could-be-the-last-straw-for-israel-and-lebanon/

[38] Aboudi, Sami and Stephanie Nebehay. 2018. “Saudi Oil Tanker Hit in Houthi Attack Off Yemen: Coalition.” Reuters, April 3. https://www.reuters.com/article/us-yemen-security-attack/saudi-oil-tanker-hit-in-houthi-attack-off-yemen-coalition-idUSKCN1HA1RT

[39] Ackerman, Gary, et. al. 2007. “Assessing Terrorist Motivations for Attacking Critical Infrastructure.” Center for Non-proliferation Studies, Monterey Institute of International Studies, Monterey, CA.

[40] Dunietz, Jesse. 2017. “Is the Power Grid Getting More Vulnerable to Cyber Attacks?” Scientific American, August 23. https://www.scientificamerican.com/article/is-the-power-grid-getting-more-vulnerable-to-cyber-attacks/

[41] Robinson, Rick M. 2016. "Cybercime-as-a-Service Poses a Growing Challenge." Security Intelligence, September 4. https://securityintelligence.com/cybercrime-as-a-service-poses-a-growing-challenge/

[42] "Physical Protection of Critical Infrastructure Against Terrorist Attacks." 2017. CTED Trends Report, March 8. United Nations Security Council Counter-Terrorism Committee Executive Directorate, New York. https://www.un.org/sc/ctc/wp-content/uploads/2017/03/CTED-Trends-Report-8-March-2017-Final.pdf

[43] "Physical Protection of Critical Infrastructure Against Terrorist Attacks." 2017. CTED Trends Report, March 8. United Nations Security Council Counter-Terrorism Committee Executive Directorate, New York. https://www.un.org/sc/ctc/wp-content/uploads/2017/03/CTED-Trends-Report-8-March-2017-Final.pdf

[44] Adam Dolnik, Understanding Terrorist Innovation: Technology, tactics and global trends (New York: Routledge, 2007), p.56. See, also, Brian Jenkins, 'Defense Against Terrorism', Political Science Quarterly 101, Reflections on Providing for "The Common Good," 101:5 (1986), pp. 777-778; Bruce Hoffman, Terrorist Targeting: Tactics, Trends, and Potentialities (Santa Monica, California: RAND 1992), p. 15

[45] Everett Rogers, Diffusion of Innovations, 5th ed. (New York: Free Press, 2003), p. 422 and Eric Abrahamson, 'Managerial Fads and Fashions: The Diffusion and Rejection of Innovations', The Academy of Management Review, 16:3 (1991), p. 592.

[46] These are adapted from the list provided in: Ackerman, Gary, "'More Bang for the Buck': Examining the Determinants of Terrorist Adoption of New Weapons Technologies" (PhD Dissertation: King's College London,2014), 23, available at: https://kclpure.kcl.ac.uk/portal/files/32901277/2014_Ackerman_Gary_0715371_ethesis.pdf, p. 12

[47] Aum Shinrikyo sought a wide array of weapons, including some high technology (and infeasible) options beyond CBRN, such as purportedly investigating an earthquake generating machine based in the work of Nikola Tesla. (Kaplan, David E., 'Aum Shinrikyo (1995)' in Jonathan Tucker (ed.), Toxic Terror: Assessing Terrorist Use of Chemical and Biological Weapons (Cambridge, MA: MIT Press, 2000), p. 212).

[48] David Ronfeldt and William Sater, The Mindsets of High-Technology Terrorists: Future Implications from an Historical Analog (Santa Monica, CA: RAND, 1981), p.14 ftn. 23. Also, Wilkinson, Paul, 'Editor's Introduction' in Paul Wilkinson (ed.), Terrorism and Technology (Portland, Oregon: Frank Cass, 1993), p. 2.

[49] Ackerman, Gary A. "Comparative Analysis of VNSA Complex Engineering Efforts." Journal of Strategic Security 9, no. 1(2016).

[50] Harry H. Turney-High, Primitive War: Its practice and concepts (Columbia, SC: University of South Carolina Press, 1949), p. 7.

[51] Warrick, Joby. 2017. "Use of Weaponized Drones by ISIS Spurs Terrorism Fears." Washington Post, February 21. https://www.washingtonpost.com/world/national-security/use-of-weaponized-drones-by-isis-spurs-terrorism-fears/2017/02/21/9d83d51e-f382-11e6-8d72-263470bf0401_story.html

[52] Rassler, Don. 2016. Remotely Piloted Innovation. West Point, NY: Combating Terrorism Center, United States Military Academy, https://ctc.usma.edu/app/uploads/2016/10/Drones-Report.pdf

[53] Gillis, Jonathan. 2017. In Over Their Heads: U.S. Ground Forces are Dangerously Unprepared for Enemy Drones. War on the Rocks, May 30. https://warontherocks.com/2017/05/in-over-their-heads-u-s-ground-forces-are-dangerously-unprepared-for-enemy-drones/

[54] Martin, P.G., N.G. Tomkinson, and T.B. Scott. 2017. "The Future of Nuclear Security: Commitments and Actions - Power Generation and Stewardship in the 21st Century." Energy Policy 110:325-330. http://dx.doi.org/10.1016/j.enpol.2017.08.038

[55] Sayler, Kelley. 2015. "A World of Proliferated Drones: A Technology Primer." A World of Proliferated Drones, June. Center for a New American Security, Washington D.C. https://www.cnas.org/publications/reports/a-world-of-proliferated-drones-a-technology-primer. Shakeel, Irfan. 2016. "Drones: The Future of Information Gathering." INFOSEC Institute General Security, August 23. http://resources.infosecinstitute.com/drones-future-information-gathering/

[56] Ackerman, Gary, Crystal Boddie, Tara Kirk Sell, Markus Binder, Matthew Watson, Anastasia Kouloganes, Rebecca Earnhardt, Hannah Collins, and Jeffrey Zboray. 2016. "Exploring the Non-State Strategic Chemical and Biological Defense Landscape: A Horizon Scan, Volume II." START, College Park, MD.

[57] Martin, P.G., N.G. Tomkinson, and T.B. Scott. 2017. "The Future of Nuclear Security: Commitments and Actions – Power Generation and Stewardship in the 21st Century." Energy Policy 110:325–330. http://dx.doi.org/10.1016/j.enpol.2017.08.038

[58] Jackson, Brian A., and David R. Frelinger. 2009. Emerging Threats and Security Planning: How Should We Decide What Hypothetical Threats to Worry About? Occasional Papers. RAND, Santa Monica, CA. https://www.rand.org/pubs/occasional_papers/OP256.html

[59] Hoodjer, Steve. 2017. "Apocalypse Not Yet: Why Adversary Unmanned Aerial Vehicles Proliferate on the Battlefield and Not in Terrorism." Master's Thesis, University of Northern Iowa.

[60] Jackson, Brian A., David R. Frelinger, Michael, Michael J. Lostumbo, and Robert W. Button. 2008. Evaluating Novel Threats to the Homeland: Unmanned Aerial Vehicles and Cruise Missiles. Santa Monica, CA: RAND,

[61] U.S. National Intelligence Council. 2012. "Global Trends 2030: Alternative Worlds." Office of the Director of National Intelligence, Washington, DC. https://www.dni.gov/files/documents/GlobalTrends_2030.pdf p. 89.

[62] Tucker, Patrick. 2017. "Counter-Terror Chief: Expect Terrorist Drone Swarms Soon." Defense One, February 27. http://www.defenseone.com/technology/2017/02/counter-terror-chief-expect-terrorist-drone-swarms-soon/135736/?oref=site-defenseone-flyin-sailthru

[63] de la Baume, Maia. 2014. "Unidentified Drones are Seen Above French Nuclear Plants." New York Times, November 3. https://www.nytimes.com/2014/11/04/world/europe/unidentified-drones-are-spotted-above-french-nuclear-plants.html

[64] "Drone Countermeasures – Hacked Off." 2016. The Economist, May 26. https://www.economist.com/news/science-and-technology/21699436-guarding-against-rogue-drones-could-be-legal-nightmare-hacked.
Popper, Ben. 2016. "This Startup Plans to Protect Airports by Taking Over Rogue Drones in Midair." The Verge, April 20. http://www.theverge.com/2016/4/20/11466368/skysafe-drones-detect-disable-protection

[65] Horowitz, Michael C. 2016. "Who'll Want Artificially Intelligent Weapons? ISIS, Democracies, or Autocracies?" Bulletin of the Atomic Scientists, July 29. https://thebulletin.org/who%E2%80%99ll-want-artificially-intelligent-weapons-isis-democracies-or-autocracies9692

[66] The "offset" strategy in military terms refers to a shift in the competitive strategic landscape during which a military takes advantage of emerging technology to gain a meaningful advantage over its opponents. The U.S. Department of Defense classifies the idea of human-machine integration as the "Third Offset" with the first being the nuclear age and the second being precision weaponry. For a brief explainer, see: Lange, Katie. 2016. "3rd Offset Strategy 101: What it Is, What the Tech Focuses Are." DoD Live, March 30. http://www.dodlive.mil/2016/03/30/3rd-offset-strategy-101-what-it-is-what-the-tech-focuses-are/

[67] Scharre, Paul and Michael Horowitz. 2015. "An Introduction to Autonomy in Weapon Systems." Working Paper, February. Center for a New American Security, Washington D.C. 5. https://www.cnas.org/publications/reports/an-introduction-to-autonomy-in-weaponsystems.

[68] Bunker, Robert J. and Alma Keshavarz. 2016. "Terrorist and Insurgent Teleoperated Sniper Rifles and Machine Guns." Open Source, Foreign Perspective, Underconsidered/Understudied Topics, August. Foreign Military Studies Office, Fort Leavenworth, KS. http://scholarship.claremont.edu/cgi/viewcontent.cgi?article=1947&context=cgu_fac_pub

[69] Rawnsley, Adam and Austin Bodetti. 2017. "Warbot Builders of the Middle East Spill Their Secrets." Wired, February 2. https://www.wired.com/2017/02/warbot-builders-middle-east-spill-secrets/

[70] Atherton, Kelsey D. 2017. "ISIS Video Shows Off 'New' Weapons Based on Old Tech." Popular Science, May 18. https://www.popsci.com/ISIS-new-weapons-old-tech

[71] Blade, Max. 2016. "Conflict Analysis: Terrorist Teleoperated Weapons Systems." Monch Publishing Group, September 1. http://www.monch.com/mpg/news/conflict-analysis/241-terrorist-teleoperated-weapons-systems.html

[72] Binder, Markus K., Jillian M. Quiqley, and Herbert F. Tinsley. 2018. "Islamic State Chemical Weapons: A Case Contained by its Context?" CTC Sentinel 11:27-31. https://ctc.usma.edu/islamic-state-chemical-weapons-case-contained-context/

[73] In the cases of the oldest digital systems, the problem of assessing cyber threats is further compounded by the scarcity of individuals who fundamentally understand their design well enough to assess vulnerability.

[74] Unfortunately, as in the case of physical security breaches, the problem of the insider attacker or cooperator remains a vexing one. Insiders might even be considered more likely in the cyber realm as physical facilitation of a cyber-attack might be seen as less extreme (not entailing any violence) and as posing a lesser risk of attribution.

[75] Franceschi-Bicchierai, Lorenzo. 2016. "The 'Danger Drone' Is a $500 Flying Hacker Laptop." Motherboard. July 28. https://motherboard.vice.com/en_us/article/xygvvk/the-danger-drone-is-a-500-flying-hacker-laptop

[76] Pato, Joseph N. and Lynette I. Millett. 2010. Biometric Recognition: Challenges and Opportunities. Washington, DC: The National Academies Press.

[77] Condliffe, Jamie. 2017. "The FBI's Facial Recognition Program is Sprawling and Inaccurate." MIT Technology Review, March 27. https://www.technologyreview.com/s/603996/the-fbis-facial-recognition-program-is-sprawling-and-inaccurate/

[78] Maze, Brianna, et. al. 2018. "IARPA Janus Benchmark – C: Face Dataset and Protocol." Paper presented at 11th IAPR International Conference on Biometrics, Gold Coast, Queensland, Australia, February 20-23. http://biometrics.cse.msu.edu/Publications/Face/Mazeetal_IARPAJanusBenchmarkCFaceDatasetAndProtocol_ICB2018.pdf

[79] Captain, Sean. 2016. "Baidu Says Its New Face Recognition Tech is Better Than Humans at Checking IDs." Fast Company, November 17. https://www.fastcompany.com/3065778/baidu-says-new-face-recognition-can-replace-checking-ids-or-ticket

[80] Jain, Anil K., Sharath Pankanti, Salil Prabhakar, Lin Hong, Arun Ross, and James L. Wayman. 2004. "Biometics: A Grand Challenge." Paper presented at International Conference on Pattern Recognition, Cambridge, UK, August. http://biometrics.cse.msu.edu/Publications/GeneralBiometrics/Jainetal_BiometricsGrandChallenge_ICPR04.pdf

[81] Goodman, Marc. 2015. Future Crimes: Everything is Connected, Everyone is Vulnerable, and What We Can Do About It. New York: Doubleday.

[82] Reproduced and revised from Gary Ackerman and James Halverson, "Attacking Nuclear Facilities: Hype or Genuine Threat?," in Brecht Volders and Tom Sauer (eds.), Nuclear Terrorism: Countering the Threat, New York: Routledge (2016), 111-141. Four cases of less relevance to the topic of this document were culled in favor of more germane cases that were discovered subsequently by the authors, these cases have been appended with individual citations.

[83] "Nuclear Successor States of the Soviet Union, Nuclear Weapon and Sensitive Export Status Report." 1994. May. Carnegie Endowment for International Peace/ Monterey Insitute of International Studies.; "Kurit-vrendo." 1993. Nuclear Threat Initiative, April 6.
http://www.nti.org/analysis/articles/kurit-vredno/

[84] Raman, B. 2006. "Mortar Attack on Pak N-facility." Rediff India Abroad. May 17. http://www.rediff.com/news/2006/may/17pak.htm

[85] "CISF Man Kills 3 Colleagues at Kalpakkam Atomic Plant." 2014. The Times of India. October 9.

[86] "German nuclear plant infected with computer viruses, operator says." 2016. Reuters. April 27.
http://www.reuters.com/article/us-nuclearpower-cyber-germany-idUSKCN0XN2OS

Disclaimer: “This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.”

World Institute for
Nuclear Security

Landstrasser Hauptstrasse 1, AT-1030, Vienna (Austria).
Tel.: +43 1 710 6519 | Fax: +43 1 710 6519 20 | Email: info@wins.org | Web: www.wins.org
International NGO under the Austrian Law BGBI. Nr. 174/1992
GZ: BMeiA-N9.8.19.12/0017-I.1/2010

WINS(18)16

ISBN 978-3-903191-17-4