CBRN Threats Short of War

Swedish resilience in a new threat environment

Inaugural speech in the RSAWS, Department VI, on March, 3rd 2020 by Ian Anthony

Resumé

Antalet fall då CBRN-material (kemiskt, biologiskt, radioaktivt och kärnämne) har använts i riktade attacker mot politiskt exponerade personer har ackumulerats till en punkt där ett systematiskt svar är motiverat. Möjligheterna till statligt engagemang i CBRN-attacker utanför väpnad konflikt indikerar att det finns problem utöver dem som orsakas av terrorism. En attack med ett avancerat CBRN-material har fortfarande låg sannolikhet, men dödligheten hos de material som används i de senaste attackerna skulle förstora effekten om en sådan händelse skulle inträffa. 2017 års nationella säkerhetsstrategi kan vägleda en respons som skulle vara en del av nationens motståndskraft, inklusive dess psykologiska dimension. En omfattande nationell kapacitet skulle vara dyr att bygga upp och internationellt samarbete bör kombineras med en effektiv användning av nationella resurser. En nationell kapacitet för förebyggande, omedelbar reaktion och återhämtning från en incident kräver institutioner, strukturer och övningar för att utveckla och testa de politiska, tekniska och brottsbekämpande dimensionerna för att möta den utmaning som CBRN-hot medför. Förfaranden för effektivt internationellt samarbete bör bl a omfatta att ta emot stöd och ge stöd till ett annat land på förfrågan. En gränsöverskridande övning med internationellt deltagande skulle vara ett effektivt sätt att testa befintlig nationell förmåga att reagera i händelse av en CBRN-attack under tröskeln för en väpnad konflikt och att identifiera luckor som måste fyllas.

MOTIVATION, INTENTION AND capability to do harm were the elements used to identify a threat during the cold war, but this traditional approach has subsequently been considered inadequate. The interpretation of threat has evolved continuously.

After the end of the cold war threats were initially disconnected from agency, and it was frequently asserted that 'the enemy is uncertainty'. The focus shifted to hazards and the risks they contain. Hazards in this context were situations containing inherent danger, and risk was seen as proportionate to the probability of the danger being realized. A crude analogy would be the hazard created by an expanse of water and risk being the likelihood that children would fall into it. The danger is latent, and it can be managed. However, the degree of danger and the level of mitigation is a matter of judgement.[1]

The growing number and increasing potency of mass impact terrorist attacks reintroduced an element of agency into thinking about threat. The presence of actors intending to do harm at scale was beyond dispute, but because the antagonists could not be identified in sufficient detail it was also difficult to understand their intentions or reveal their capabilities. Unable to find a decisive point of attack, the priority became keeping up

with an agile and constantly evolving enemy able to revise his organisation and change his tactics in ways that are hard to predict.

The response to mass impact terrorism cemented an already emerging awareness that developments taking place at a distance could have local impact. Far away conflicts that displaced large numbers of people, created safe havens for terrorists or incubated extremist views leading to violence could quickly translate into national security threats. By extension, addressing issues such as fair and equal treatment of minority populations or women and men became not only matters of political interest but also part of threat mitigation.

The use of military force by states inside Europe to bring about outcomes that could not be achieved by peaceful means returned the element of agency to European threat assessments. Major conflicts have been fought at roughly six-year intervals on the territory of the former Soviet Union, and a wider conflict drawing in many European states is no longer excluded. While it is not predicted, or considered a high probability event, a wider European conflict out has become a planning assumption for many states.

A scan of current public assessments by responsible authorities underlines that Russia and Western countries use each other as the yardstick for measuring threat. However, a contemporary understanding of threat includes muscular forms of competition that do not fit into a binary model of peace or war. Competition with a military dimension below the level of armed conflict has become one focus for security planning.[2]

What does resilience mean in this context?

Increasingly complex societies present an enormous, and continuously expanding, target set for malicious actors. Meanwhile, the Covid-19 pandemic has provided an unwelcome reminder of the damage that general hazards may cause. Low probability but high impact events will sometimes occur, and a degree of preparedness is necessary.

The term 'structural vulnerability' has been used to capture the reality that contemporary threats can not be defeated in a comprehensive manner.[3] Structural vulnerability is now an enduring, if not permanent, feature of national, international and collective security. In response the Swedish National Security Strategy draws attention to the need for 'the collective resilience of society'.[4]

As incorporated into the National Security Strategy resilience includes capabilities that can be mobilized to prevent a threat arising and to address a threat as it unfolds.[5] From a Swedish perspective resilience should therefore also include a method for anticipating what might happen, and a system to translate anticipation into prevention.

A risk informed approach is needed to plan, prepare and respond to possible contingencies in proportion to their potential consequences, understanding that risks can never be eliminated, only reduced.

The Covid-19 pandemic has probably sensitized Swedish society to the idea that the task of public policy is to reduce risk to acceptable levels. However, a threat picture in which no comprehensive defence is possible against an expanding number of potentially negative contingencies is difficult for a society that has enjoyed roughly three decades of more or less uninterrupted peace to assimilate. The need for a psychological dimension within resilience is noted in the National Security Strategy.[6]

Elements of a contemporary Swedish threat assessment

The Swedish National Security Strategy contains a taxonomy of threat, even if it is not presented as such.

Hazards that present a *general or global threat* are reflected in the attention drawn to the potential negative impact of changes in climate, environment and resource availability.[7]

As a country that depends on a stable basis for international cooperation on equitable terms, Sweden will be particularly concerned by *threats to principles and regimes*.[8]

No state has the resources to address structural vulnerability in a comprehensive way, and international cooperation is an important element of national planning. Sweden has built its international cooperation on full compliance with agreements. Failing to live up to commitments freely given would be a *threat to reputation* that would damage Swedish interests more broadly.

The *direct, physical threat* to Sweden is recognized in the preface to the document, where the text speaks of primary threats against which the Swedish people must be protected, and in the need to strengthen both military capability and civil defence.[9]

There is a *cross-domain threat* to Sweden in an era of 'muscular competition'. The annual report of Swedish military intelligence draws attention to the transition from a linear crisis/escalation/conflict paradigm to a non-linear capacity to increase or decrease the levels of conflict across various domains, of which armed attack is only one (albeit the most serious).[10]

Since Swedish interests are distributed around the world, there is also an *indirect physical threat* to companies, citizens and supply chains.

There is an implicit geographical prioritization in the National Security Strategy. Since events around the globe can have local impact, attention to *remote threats* is a national interest. However, *neighbourhood threats* are considered a higher priority given that Swedish interests 'are particularly closely integrated with Nordic and Baltic neighbours, with the EU and the wider Europe.'[11]

To safeguard societal functions that are important to meeting citizen needs the *threat of accident* needs to be taken into account alongside threats posed by adversaries.[12]

Recent cases of CBRN use: threats and challenges

During the cold war the general threat posed by chemical, biological and nuclear weapons was a constant feature of strategic analysis. To what degree do chemical threats challenge the Swedish approach to resilience?

It is worth noting that the military utility of chemical weapons is still a relevant consideration even though huge quantities of chemical weapons previously available for battlefield use at very short notice during the cold war have been destroyed.[13]

The general threat posed by chemical weapons has received greater international attention following their confirmed use on the battlefield in Syria, where chemical attacks attributed to the Syrian armed forces were a feature of urban warfare. The use of a sophisticated and highly lethal chemical agent in Europe is a reaffirmation that CW research, development and production facilities still exist in spite of the major disarmament effort.

A catalogue of recent incidents involving the use of CBRN materials in targeted attacks on politically exposed individuals has made the threat more tangible in recent years.

The former President of Ukraine, Viktor Yushchenko, was poisoned while running for office in December 2004. In November 2006 a former Russian intelligence officer, Alexander Litvinenko, died in London after ingesting a highly radioactive isotope of polonium. In early 2017 Kim Jong Nam (half brother to the ruler of North Korea, Kim Jong Un) was killed in Malaysia after being attacked with a nerve agent. In March 2018 a former Russian intelligence officer, Sergey Skripal, and his daughter Julia fell seriously ill after being poisoned with a nerve agent. Three months later two UK citizens were exposed to the same chemical and one of them died.[14] In August 2020 the Russian politician Alexei Navalny fell seriously ill after being poisoned with a nerve agent belonging to the same family of chemicals used to attack the Skripals.

The reopening of an investigation in Bulgaria into a death with what appear to be characteristics in common with the Salisbury attack can perhaps be added to the list, as well as the 2004 death of Yasser Arafat, former Chair of the Palestine Liberation Organisation, aspects of which remain unexplained.

There is not space to address each incident in detail, but it is possible to draw attention to some features that justify addressing the threat that they pose in a systematic way.[15]

In each case the *potential motive* for an attack points to state involvement. Where chemical attacks have been attributed to non-state actors, incidents have usually involved industrial chemicals that are widely available and relatively easy to obtain.[16] The attacks listed above were carried out with *sophisticated and highly lethal man-made materials* that are not widely available.

Attacks occurred in places where *the public was inevitably exposed* to a highly toxic substance, even when *the means of delivery was very directly targeted* on a specific individual. If they had been used in a different way the more lethal of the chemical agents could have caused casualties on a scale that might *overwhelm the public health response*.

The *means of delivery was unorthodox*, not employing a weapon as traditionally defined. Poison was administered in food, smeared onto the skin of the target, or the clothes of the target may have been deliberately contaminated.

Issues raised by the targeted attacks

It is also not possible to pick up all relevant aspects arising from the incidents of targeted attack in this article, only to touch on some salient points related to prevention; the immediate response to an attack; restoring the location of an attack to the point where it is safe for the public; identifying the perpetrators of an attack; conducting a criminal investigation perhaps leading to prosecution; and the political dimension of organizing a response.

Prevention

It was not possible to prevent the attacks even though the targets were known to be at risk and, in the case of Yuriy Skripal, under the protection of a state host. Attackers were able to travel to his home without being detected on the way into or out of the country.

Quite a lot of information about the attack on Mr. Skripal has been made public, but the authorities have maintained silence on how the nerve agent was transported to the place where the attack took place. The Polonium-210 that poisoned Alexander Litvinenko has characteristics that helped authorities trace the pathway it followed across Europe. The material travelled from Moscow

to London via Hamburg. However, the material was not detected prior to an attack.

The individuals subsequently identified as primary suspects in carrying out the attack on Mr. Litvinenko and Mr. Skripal were known to be employees or former employees of the Russian intelligence services, but as far as open sources tell they arrived in the UK and travelled freely without surveillance.

First response

In several cases there was some delay before it was understood that an attack may have involved the use of CBRN material. It took many years before the death of Yasser Arafat was investigated as a possible poisoning with highly radioactive material and three months before independent toxicology tests were carried out on Viktor Yushchenko.

It appears that public health authorities and first responders in the UK were more sensitive to the possibility that a casualty may have been the victim of a CBRN attack. In the Litvinenko and Skripal cases a police officer connected information obtained during a general briefing on CBRN issues when listening to a medical professional describe symptoms. The training and alertness of police officers played a part in triggering a CBRN response.

A combination of techniques (interviews, investigating the movements of persons of interest, telephone records, seizing and viewing closed circuit television (CCTV) footage) established that CBRN material may be present in many locations and not only in the place where the attack took place.

The possibility that many public places were contaminated with a highly toxic substance triggered wide-area tracing linked to the specific characteristics of the CBRN agent.

The chemical agent used to attack Mr. Skripal is highly toxic when in contact with skin. A policeman who touched the door handle at the Skripal's house was hospitalized and subsequently retired from police service on medical grounds. A couple living in a village several miles away from the original attack site were exposed to the agent and one of them died. Before becoming so ill that he collapsed, Mr. Skripal ate in a restaurant and walked in a park. Therefore, a large public space was designated as a hazard that might contain dangerous levels of contamination.

Once it was known that Polonium-210 was used to poison Mr. Litvinenko it was possible to scan for its presence, which was discovered in multiple places around the London borough where he lived. The health risks associated with Polonium-210 are associated with ingestion or inhalation, meaning that a relatively small area (the building where Litvinenko lived) was considered a hazard, but a large part of a densely populated London borough became part of a crime scene.

Managing the locations associated with an attack raised issues of how to safely handle items that might be contaminated with a highly toxic agent when the same items could also hold forensic information needed as evidence in a subsequent criminal case.

Site recovery

Clean-up operations can be expensive and time consuming when highly toxic CBRN agents are present.[17] For reference, the cost of decontaminating two apartments in a cesium-137 poisoning case in Germany has been put at €2.5 million.[18]

The scale of clean-up operations require a political decision informed by technical information. For example, a public park in Salisbury represented a hazard in that it might be contaminated with traces of a

highly toxic chemical. At the same time, the risk might be lowered by the small probability that a member of the public would come into contact with the chemical. A different calculation of risk might be reached if the hazard was present in, for example, a restaurant or café where a more extensive clean-up would be necessary.

In the case of Mr. Skripal the political instructions given to responsible agencies shaped the cost and time of clean-up operations. It was known to the public that the chemical agent used in the attack was extremely lethal even in millilitre quantities. The political instruction was to clean the environment to the point where there was zero risk to the public.

A message of zero risk could be considered reassuring to a concerned public, but it imposed a huge volume of work on responsible authorities tasked with searching large public spaces to find minute traces of a chemical.

The task of carrying out clean-up was delegated to a specialized unit within the armed forces. However, the specific task was not the one they were trained and equipped to carry out. The military units were expert at decontaminating hard surfaces (such as armoured vehicles) to a level where they could return to the battlefield. In that contingency military personnel would have immediate access to protective equipment, further reducing the probability of exposure, and would be expected to accept a higher degree of risk than could be imposed on civilians.

In Salisbury units were tasked to decontaminate buildings full of soft surfaces against a more demanding standard applied to the general public. Where it was decided that decontamination was impossible items needed to be safely transported to a site where they could be destroyed without damage to the environment. Specialized contractors with experience of handling hazardous materials were required to carry out that task.

In 2017 the British government explained that after a deliberate CBRN attack building owners or occupiers would be responsible for meeting the cost of decontaminating their property, while local authorities would be responsible for public buildings, public spaces and amenities.[19] However, following the attack in Salisbury the assets of civilian owners (and local government authorities) were confiscated and destroyed without a clear understanding of how insurance or other compensation claims would be affected. More broadly, significant parts of Salisbury were completely closed to the public for up to three months with a financial impact on businesses inside the perimeter.

The UK was forced to address the issue of whether a unit within the armed forces should respond to a domestic incident where a state used an advanced CBRN material outside an armed conflict.[20] Should the capability of the military unit be adapted or should the task be placed elsewhere, for example in a specialized police unit or a civilian emergency response unit?

Attribution

The inquiry into the death of Alexander Litvinenko found 'a strong circumstantial case that the Russian State was responsible for Mr Litvinenko's death'.[21] In relation to the attack on Mr. Skripal the UK Prime Minister announced that 'the Russian Federation was responsible for an attempted murder here in our country' and that there was 'no other plausible explanation'.[22]

In each case attribution partly rested on technical evidence derived from forensic analysis of the material used in an attack. The very special characteristics of Polonium-210 (and later the Novichok nerve agent) nar-

rowed the scope of the potential sources of supply. However, forensic analysis was not sufficient by itself for attribution.

The United Kingdom has specialized facilities that could analyse the CBRN material used in attacks. The analysis of blood and urine samples at the Atomic Weapons Establishment (AWE) established the presence of Polonium-210 in the Litvinenko case. A highly qualified UK academic scientist stated in media interviews that the characteristics of the Polonium-210 should be sufficient to attribute the attack. However, the Litvinenko inquiry concluded that although the Polonium-210 certainly could have been produced in a Russian reactor, it was not possible to say on the basis of purely technical evidence that it 'either must have come, or even probably came, from Russia'.[23]

The Defence Science and Technology Laboratory at Porton Down, UK, was able to analyse samples in the Skripal case. In addition to blood and tissue samples a quantity of the chemical agent itself was recovered from a site a few kilometres away from the place where Mr. Skripal was attacked. In this case forensic chemical identification and analysis was able to identify the chemical agent used but could not establish a unique 'fingerprint'. The agent was almost entirely free from the distinctive impurities that would normally be a by-product of industrial production.

The almost complete purity of the Polonium-210 and the Novichok agent helped investigators to conclude with high confidence that the materials were produced in government laboratories and led to the general characterisation of the Novichok as 'military grade'.

The UK has highly specialized laboratories with extensive knowledge of CBRN materials, but these technical assets were not sufficient by themselves to attribute an attack. For attribution forensic analysis was combined with normal police work to assess motive, opportunity, the identity and movements of persons of interest before and after the attacks took place and so on. However, when attributing an attack to a foreign state the standard applied was based on the 'balance of probabilities', not the standard that would have been applied in a criminal case of 'beyond reasonable doubt'.

Attribution was not driven by technical agencies or by the police, though both played a key role in the process. The driver of attribution was a political body—the specialized national security apparatus established under the Cabinet Office that was able to pull together relevant authorities from across different parts of national and local government as well as specialized technical agencies.

Criminal investigation and prosecution

The United Kingdom treated the attacks on Mr Litvinenko and Mr. Skripal as murder and attempted murder even though attribution to a foreign state also made the issue a matter of national security policy.

The reference to criminal law required the indictment of specific individuals and the collection of evidence that would meet the standard required by a court. In the Litvinenko case three weeks passed before blood and tissue samples were analysed by AWE. More importantly perhaps, more than two months passed before some of the surfaces in buildings where suspects were present along with Polonium-210 were tested. Meanwhile, surfaces had been cleaned multiple times. Delays and contamination of crime scenes could reduce the value of forensic evidence in a court proceeding.

At crime scenes the handling of items that were both hazards and evidence in a criminal

case requires agreement between relevant authorities on standard operating procedures. These issues have been thoroughly explored in relation to mass impact terrorism.

There is an important role for prosecutors in designing a system to respond to CBRN incidents. The resources available for a criminal investigation are linked to the potential for a successful prosecution, and a prosecutor is unlikely to support a case that they don't consider winnable. Prosecutors need to be sensitive to which parts of the criminal law are applicable and work with legislators to ensure that offences are defined. Investigative bodies must have the powers and the knowledge needed to produce a case file that the prosecutor can make use of.

Cross-border and international cooperation is likely to be an essential element of building a case. The greater resources being devoted to CBRN issues by e.g. the International Criminal Police Organization (INTERPOL) suggest that the cross-border dimension of future investigations could become more effective in future cases.

Political response

After attributing an incident to a foreign state, the use of CBRN in targeted attacks was brought to the table in a range of international organizations and frameworks. The increased attention to targeted attacks has led to a progressive escalation in the severity of the international response.

In 2018 a group of 40 states and the European Union came together in an International Partnership against Impunity for the Use of Chemical Weapons that has harmonized lists of legal and physical persons that are subject to targeted sanctions because of their connection to chemical weapon attacks.

The European Union imposed sanctions on the individuals identified as suspects in the criminal investigation of the Skripal attack, and to senior figures in the Russian security establishment believed to have played a role in poisoning Mr. Navalny. Seven members of the Russian delegation to NATO were expelled, and accreditation was refused to others in response to the Skripal case.

The G7 Foreign Ministers expressed support for the UK finding of Russian responsibility for the Skripal attack and called for a criminal investigation into the poisoning of Mr. Navalny.

The attack on Mr. Skripal was raised in the UN Security Council, which held several inconclusive meetings to discuss its implications. European members of the UN Security Council raised the poisoning of Mr. Navalny during a period when Russia was President of the Council. The Russian government was pressed to investigate the poisoning and to report the results of the investigation to the Security Council.

Russian authorities requested a technical assistance visit by a team of OPCW experts in October 2020 and bilateral discussions explored the legal, technical, operational, and logistical parameters of such a visit. However, the OPCW concluded that the Russian request would not meet the necessary requirements for assistance and no visit took place.[24] This issue was prominent in discussions at the twenty-fifth Conference of States Parties to the CWC in April 2021.

The degree of coordinated international action being mobilized underscores the opposition to the use of chemical weapons in any form, and that attacks on individuals with CBRN materials can be considered a threat to international peace and security. However, the problems encountered in finding a common approach to addressing the new threats at the UN Security Council and in the framework of the CWC also highlight the limitations of the existing multilateral

mechanisms when faced with a new and unanticipated challenge.

Managing the political impact of the public narrative surrounding an attack

The attacks using CBRN materials underscore the changing role of the media and the influence of social media in shaping a wider political narrative. In a democratic society with a free media, authorities with incomplete information—some of which might subsequently turn out to be incorrect—must make an immediate public response to an incident.

One feature of recent attacks has been the tendency for alternative theories that purport to explain an incident to circulate in public almost immediately. Following the Skripal attack, for example, a Danish researcher traced more than thirty alternative explanations for the events in Salisbury, UK published in Russian media outlets.[25]

A second feature is a coordinated effort to question or discredit information on which attribution is based. Where attribution was based on balance of probabilities the lack of 'proof' beyond reasonable doubt was used to question who was responsible.

A third feature is 'what aboutism'—assertions that even if an incident did occur, it is similar in kind to actions undertaken by the accuser. Criticism of an attack on the basis of its legality is thereby painted as hypocritical and motivated by political rather than rule of law factors.

Informing the public in the face of active disinformation is one contemporary challenge, the pace of the modern news cycle is another. Political decision makers will be pressed to explain how they plan to respond to an incident in 'real time', before they have had a chance to assimilate and evaluate information. Furthermore, the option of 'quiet diplomacy' that existed when information could be controlled more effectively may no longer be available. The risk that an attack will rapidly escalate into a crisis is therefore increased if responding to pressure for a rapid response promotes a narrative based on spiraling sanctions or reprisals.

The relationship between the media and non-governmental experts has also become a factor in establishing a public narrative around an incident. Comments by non-governmental scientists who are undoubtedly expert in their field have sometimes complicated the development of an authoritative official version of e

Sweden – Threat and Resiliation

The accumulation of cases when CBRN material has been used in targeted attacks against politically exposed persons has motivated Western states to begin organizing a systematic response. An effective, systematic Western response would become an element of Swedish resilience, including its psychological dimension. The taxonomy of Swedish national security threat assessment can guide and organize actions and ensure that Sweden will play its proper role in helping to develop a systematic response.

- *General or global threat* — The case in Malaysia indicates that CBRN attacks on politically exposed persons are not limited to Europe. Drawing attention to the targeted killing of political opponents would raise the profile of an emerging general threat to international order.
- *Threats to principles and regimes* — Slowing or reversing the erosion of the legal framework prohibiting any use of chemical weapons and legal instruments to ensure biological, nuclear and radio-

logical security is essential to underpin resilience.

- *Threat to reputation* — Sweden has positioned itself as a champion of multilateral rules. Failing to implement existing rules nationally would cause damage to reputation.
- *Direct, physical threat* — Targeted killings have not caused large-scale mortality or mass casualties, but an agent such as 'Novichok' could do so if used in a different way. Recent cases indicate that attacks can cause severe disruption and that there is a high financial cost to recovery. The use of a sophisticated hazardous material in, for example, the chief financial district or a major transport hub would rise to the level of a national emergency.
- *Cross-domain threat* – Attacks with specialized hazardous materials could form part of a set of non-linear incidents that are connected, but at the same time deniable, hidden or ambiguous incidents. National security preparations need to consider the full spectrum of possibilities.
- *Indirect, physical threat* – Attacks in countries other than Sweden could damage the assets of Swedish companies or their commercial activities if key supply chains are disrupted or business partners suffer. Working with key international partners is an important element of national preparedness.
- *Remote threat* – The inter-connectedness of economies and societies along with the rapid spread of information (and disinformation) through modern communications can produce a local political effect from an event anywhere in the world.
- *Neighbourhood threat* – The impact on Sweden of an incident in the immediate neighbourhood (principally in a Nordic-Baltic state) would be proportionately much greater than an incident further away.
- *Threat of accident* – Many CBRN materials represent a hazard in which threat is latent. The safe and responsible handling of materials in commercial and scientific use reduces physical threat, and it is an element of psychological resilience because it is reassuring to the public.

Lessons from abroad to promote national preparedness

The United Kingdom developed an extensive CBRN national response system prior to the Litvinenko and Skripal attacks. However, although a great deal of thought had gone into designing a national system, not all of the issues arising from a real attack could be addressed within the established framework.

The UK system was tailored to counter-terrorism, and state involvement introduced additional dimensions and altered the context for organizing a response. For example, the nature of the CBRN materials available to even sophisticated terrorist groups would be different from those used in recent attacks. A second example, a state disinformation campaign to complicate attribution or blunt the political response after an attack can be more sophisticated and more sustained than anything a terrorist organization could implement. The responsibility of central government, local government, insurance companies and property owners in meeting the cost of recovery after an attack was another area where arrangements fell short of what was needed.

A focused bilateral discussion with partners in the United Kingdom would be justi-

fied to understand in greater detail lessons that have been learned from recent attacks and how they might apply in Sweden.

Regular exercises using different scenarios would be a means to develop a comprehensive national response plan across the spectrum of different CBRN threats. Scenarios to test the reaction to CBRN threats involving state actions short of war could be built into the calendar of exercises that bring together intelligence and security personnel; operational personnel (such as frontline officers and first responders); investigators and prosecutors; policy, legal and regulatory subject matter experts; and technical experts.

The importance of shaping a political context and trying to control the narrative around an incident was noted above. Public messaging should be harmonized with operational guidelines so that there is a clear understanding of the level of acceptable risk and general understanding of the basis on which decisions have been taken. A national exercise should include participation by political decision-makers and their advisers at national and local level.

Political leaders also need to consider how risk assessment is translated into instructions given to the agencies responsible for implementing a response based on a knowledge of the cost and time implications associated with different options.

Exercises of this kind would pinpoint existing national capabilities as well as the capabilities that are necessary but missing. The degree to which the national legal framework is in place, the lines of communication among authorities and the extent to which information can be shared would also be revealed in exercises.

It is very unlikely that all of the necessary elements of a national response plan exist, or that generating a comprehensive capability based entirely on own resources would be proportionate to the threat. An exercise can help determine which missing capabilities should be developed nationally, and which should be sought through international cooperation.

Promoting international cooperation

The mass impact terrorist attacks in the United States in September 2001 accelerated the international discussion of counter-terrorism, including the potential use of CBRN materials. The European Union has launched a series of initiatives to address CBRN terrorist threats both outside and inside the EU. The most recent CBRN Action Plan focused on EU internal security dates from 2017 and continues to emphasize possible terrorist attacks.[26]

Targeted assassination attempts with highly specialized CBRN materials not normally in commercial use differentiate the recent incidents from terrorist attacks, for which a great deal of preparation has already been made. The compatibility of a national plan with the arrangements being made in neighbouring states would be a first step in addressing the cross-border and international dimension of a response. Sharing good practice and the systematic organization of knowledge in the immediate neighbourhood could promote a sustainable regional response based on local capabilities.

A further step would be to consider harmonization of response plans with a wider EU dialogue to promote cohesion and integration and to direct common resources. There is a strong case for revisiting the EU CBRN Action Plan to consider where revisions are needed to take account of a changing threat environment.

The specialized nature of the CBRN materials used in recent targeted attacks inevita-

bly raises the question of state involvement. Political leaders need to consider how they will respond in international forums to an attack that takes place on national territory or when national territory is used to prepare for or carry out an attack elsewhere. To arrive at a coordinated, collective response in a timely manner the issue should be on the agenda when responsible ministers from different like-minded states meet.

The possibility that criminals are acting on behalf of a foreign state has been an element of combating mass impact terrorism. Organizing a public safety response alongside crime scene management when an incident has national security implications is a complex problem, but one that has usually involved a proxy actor rather than direct action by officers of a state.

Building a national capacity to analyse samples of different kinds of material should be balanced with international cooperation among states and between states and specialized institutions. Sweden already has important laboratories that played a valuable role in the technical analysis of chemical agents following recent attacks, at the request of the OPCW. The OPCW is now preparing to build a new facility, the ChemTech Centre, and how states can work with and make use of that new resource is yet to be explored.

Law enforcement authorities, including INTERPOL, are now focusing more of their resources on investigating CBRN incidents, raising new questions for prosecutors and judges should investigations lead to court cases, or if investigators are asked to support an investigation in another state.

In the response to a CBRN attack the specialized agencies tasked with cleaning the environment and restoring public places for safe use must consider whether they have the operating procedures, equipment and training to cope with materials that they will never normally come across in their work.

A national exercise with international participation designed to identify gaps in the capability to respond to a CBRN attack short of war can be the first step in designing systematic protection. The outcome would be a valuable input to a national response plan to meet the challenge posed by CBRN threats short of war to underpin a new iteration of the national security strategy.

The author is Dr. and the Programme Director for European Security at SIPRI and a fellow of RSAWS.

Notes

1. Braun, Herbert: "The non-military threat spectrum" in *Armaments, Disarmament and International Security*, SIPRI Yearbook 2003, Oxford University Press, Oxford 2003, pp. 33–43, *https://www.sipri.org/yearbook/1993*.
2. OSCE High Level Military Doctrine Seminar: Opening Remarks by General Tod D. Wolters, 2021-02-09.
3. Cornish, Paul: "NATO: the practice and politics of transformation", *International Affairs*, vol. 80 no. 1, 2004.
4. *Nationell Säkerhetsstrategi*, [National Security Strategy], Regeringskansliet, January 2017, p. 14, *https://www.regeringen.se/48db21/globalassets/regeringen/block/aktualitetsblock/statsradsberedningen/nationell-sakerhetsstrategi.pdf*.
5. Ibid., p. 9.
6. Ibid., p. 17.
7. Ibid., p. 10.
8. Ibid., p. 16.
9. Ibid., p. 3, p. 15.

10. *MUST Årsöversikt 2020* [MUST Annual Report 2020], Military Intelligence and Security Service, Swedish Armed Forces, February 2021, *https://www.forsvarsmakten.se/siteassets/4-om-myndigheten/dokumentfiler/rapporter/must-arsoversikt-2020.pdf*.
11. Op. cit., *Nationell Säkerhetsstrategi*, see note 4, p. 6.
12. Ibid., p. 14.
13. The destruction of roughly 70,000 tonnes of chemical agent has been verified by the Organisation for the Prohibition of Chemical Weapons (OPCW) since the entry into force of the Chemical Weapons Convention (CWC). *Report of the OPCW on the Implementation of the Convention on the Prohibition of the Development, Production, Stockpiling and Use of Chemical Weapons and on their Destruction in 2019*, OPCW, The Hague, 2021-04-20.
14. Anthony, Ian and Fei, Su (eds.): *Reassessing CBRN Threats in a Changing Global Environment*, SIPRI, June 2019, *https://www.sipri.org/sites/default/files/2019-06/1906_cbrn_threats_su_anthony_0.pdf*.
15. Toprak, Sadik: "Trends in recent CBRN incidents" in ibid.
16. A notable exception was the use of Sarin gas in the 1995 attack in Tokyo. Okumura, Tetsu; Taki, Kenji; Suzuki, Kouichiro and Satoh, Tetsuo: *The Tokyo Subway Sarin Attack: Toxicological Whole Truth*, *Handbook of Toxicology of Chemical Warfare Agents*, Academic Press, London 2009.
17. "The social and economic impact of chemical weapons attacks", *Integrity Initiative*, 2019-05-15, *https://medium.com/@hitthehybrid/the-social-and-economic-impact-of-chemical-weapons-attacks-aff310861942*.
18. "CSI Karlsruhe: Nuclear forensics sleuths trace the origin of trafficked material", *Actinide Research Quarterly*, Los Alamos National Laboratory, 4th quarter 2007, pp. 1-9, *https://www.lanl.gov/discover/publications/actinide-research-quarterly/pdfs/ARQ-2007-12.pdf*.
19. *UK Government Decontamination Service, Strategic National Guidance*, March 2017, p. 12, *https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/622617/SNG_5thEdition_Final_March_2017__1_.pdf*.
20. "Welcome back 28 Engineer Regiment and British Army control of CBRN", *British Armed Forces Review*, 2019-04-01, *https://britisharmedforces-review.wordpress.com/2019/04/01/welcome-back-28-engineer-regiment-and-british-army-control-of-cbrn/*.
21. The Litvinenko Inquiry: Report into the death of Alexander Litvinenko, Presented to Parliament pursuant to Section 26 of the Inquiries Act 2005, 2016-01-21, *https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/493860/The-Litvinenko-Inquiry-H-C-695-web.pdf*.
22. PM Commons statement on National Security and Russia, The Prime Minister's Office, UK Government, 2018-03-26, *https://www.gov.uk/government/speeches/pm-commons-statement-on-national-security-and-russia-26-march-2018*.
23. Op. cit., The Litvinenko Inquiry…, see note 21, p. 225.
24. *Opening Statement by the Director-General to the Conference of States Parties at its Twenty-Fifth Session*, OPCW document C-25/DG.22, 2021-04-20.
25. Hansen, Flemming Splidsboel: *Russian Disinformation: An example*, Danish Institute for International Studies, 2019.
26. *Action Plan to enhance preparedness against chemical, biological, radiological and nuclear security risks*, European Commission, Brussels, COM (2017) 610 final, Brussels, 2017-10-18, *https://ec.europa.eu/home-affairs/sites/default/files/what-we-do/policies/european-agenda-security/20171018_action_plan_to_enhance_preparedness_against_chemical_biological_radiological_and_nuclear_security_risks_en.pdf*.