FREEDOM FROM FEAR
M A G A Z I N E

F³

THE PAST, THE PRESENT AND THE FUTURE... IN OUR HANDS!

Chemical, biological, radiological and nuclear risk mitigation

unicri
United Nations
Interregional Crime and Justice
Research Institute

GHENT UNIVERSITY

FREEDOM FROM FEAR
M A G A Z I N E

THE PAST, THE PRESENT AND THE FUTURE... IN OUR HANDS!

Chemical, biological, radiological and nuclear risk mitigation

CONTENTS

ii

Chemical, Biological, Radiological and Nuclear Risk Mitigation: A Model for Community-Driven Responses

by Antonia Marie De Meo
Director of UNICRI

At the beginning of the COVID-19 pandemic, UNICRI celebrated the 10th anniversary of the Chemical, Biological, Radiological, and Nuclear (CBRN) Centers of Excellence risk mitigation programme, generously funded by the European Union. This initiative brings together stakeholders from 62 countries at the international, regional, national, and local levels to cooperate in CBRN security governance and to promote a global culture of safety and security.

Against the backdrop of the COVID-19 pandemic – the biggest crisis of our lifetime – the threat posed by dangerous CBRN agents and materials remains high, with special need to focus attention on biological threats. Criminal elements are taking advantage of vulnerabilities in society exposed by the COVID-19 pandemic.

Moreover, terrorists may misuse potential CBRN agents, which is a serious concern for governments and a threat to civilian populations worldwide.

The CBRN field is prone to fragmentation, with each sector – chemical, biological, radiological, and nuclear – often studied in isolation. When this occurs, it is counterproductive, because coordinated resources, expertise, and authority are needed to address all aspects of CBRN risks.

Each of our 62 partner countries voluntarily participates and takes ownership over the CBRN work, which has contributed to the success of the responses to the biological threat posed by the COVID-19 pandemic. Ten years ago, this approach generated skepticism, especially from those who believed that there could not be adequate commitment in the absence of a politically or legally binding agreement. However, voluntary participation has proven essential to ensuring that partner countries are owners of the initiative. And their ownership can be seen in the manner in which the 62 countries that are part of the CBRN Centers of Excellence have responded to the pandemic.

During COVID-19, partner countries identified their priority needs. Our decentralized

CBRN Centers of Excellence Regional Secretariats then worked with partner countries to ensure that available expertise was mobilized to respond to their specific needs, thereby reducing the impact of the pandemic in their communities. For example:

▸ In Africa, more than 1500 people benefited from a door-to-door awareness raising campaign and distribution of masks, as well as in-person trainings on safe and dignified burial and webinars on COVID-19 risks related to wastewater;

▸ In Eastern and Central Africa, the CBRN Centers prepared a joint roadmap for 2021;

▸ In the Gulf Cooperation Council Countries, a Regional CBRN Training Hub was inaugurated with Abu Dhabi University;

▸ In the Middle East, the CBRN Centers supported Lebanon in the aftermath of the tragic Beirut explosion to identify critical priorities and respond to emergency needs;

▸ In Central Asia, the CBRN Centers purchased necessary equipment for front-line officers to protect them from COVID-19; they also conducted awareness raising campaigns for university students;

▸ In South East Asia, they focused on peer-to-peer sharing of knowledge and experience on COVID-19; and

▸ In South East and Eastern Europe, partner countries came together to combat the spread of COVID-19 in a coordinated manner.

By adopting a flexible, country-drive approach to CBRN risks, UNICRI has also been able to take a whole of society approach by including women and youth and ensuring no one is left behind. For example, in Central Asia and Eastern Europe, a large number of female scientists shared their expertise in diagnostic medicine related to the COVID-19 pandemic response. We also partnered with the local community in Uzbekistan to host a drawing competition for schoolchildren, which raised their understanding of bio-risks, such as a coronavirus outbreak.

UNICRI's example of the CBRN Centers of Excellence concretely prevents CBRN risks by promoting good governance, a culture of safety and security, cooperation, and the transfer of best practices. We learn together and we become more effective together to achieve our ambitious goal of promoting healthy, peaceful, and inclusive societies for sustainable development.

Building upon the forward-thinking, learning, and achievements of the CBRN programme, UNICRI has a new programme, CONTACT, which was launched with the generous support of the Governments of Canada, Norway, United Kingdom and United States. CONTACT is one of UNICRI's flagship programmes in nuclear security. It enhances capacities of state security, law enforcement and other agencies to carry out intelligence operations aimed at thwarting trafficking of radiological and nuclear (RN) materials. CONTACT focuses on fostering regional cooperation and exchange of information on RN trafficking investigations. Since its inception, CONTACT has involved countries in the Middle East, Black Sea and Southeast Asia regions.

In cooperation with UN-OCT-UNCCT, UNICRI has also recently launched the new report "Advances in Science and Technology to Combat Weapons of Mass Destruction (WMD) Terrorism". The report is an output of the United Nations Global Counter-Terrorism Coordination Compact Working Group on Emerging Threats and Critical Infrastructure Protection project on Technology and Security: Enhancing Knowledge about Advances in Science and Technology to Combat WMD Terrorism, which is funded by UNOCT-UNCCT and co-implemented with UNICRI. The Working Group promotes coordination and coherence to support Member States to address emerging terrorist threats, including those related to CBRN materials.

The threats derived from the misuse of CBRN agents and materials know no boundaries, which makes international cooperation critical. COVID-19 serves as a devastating reminder of this in the sector of biorisks. In these extremely challenging times, when people all around the world are experiencing health, economic, and social crises simultaneously, the UNICRI CBRN programme has proven to be an effective network for international cooperation based upon a common understanding of risks and a global commitment to jointly share responsibilities. UNICRI is on the front line with partner countries, facilitating priority responses to limit the negative consequences of the pandemic, and supporting Member States to plan for recovery as the pandemic subsides.

A key lesson learned from the CBRN programme is the importance of protecting communities. Awareness of CBRN risks must be raised across the public at large, starting in local communities with CBRN stakeholders and extending to community leaders, NGOs, media, universities, students, and parents.

This issue of the Freedom From Fear Magazine focuses on CBRN risk mitigation to honor the victims of CBRN catastrophes, who guide us in our quest for lasting peace and security.

> "When we see the Earth from space, we see ourselves as a whole. We see the unity, and not the divisions. It is such a simple image with a compelling message; one planet, one human race.

Stephen Hawking

v

FACING TODAY'S BIORISKS

THE WORK OF THE UNITED NATIONS BIORISK WORKING GROUP (UN-BRWG): TOWARDS ACTION IN STRENGTHENING THE INTERNATIONAL COMMUNITY'S RESPONSE AND IN IMPROVING PREVENTION

Interview with: Mike Ryan, Executive Director of the World Health Organization Emergencies Programme and Izumi Nakamitsu, Under-Secretary-General and High Representative for Disarmament Affairs

by Francesco Marelli

WHAT CAN COVID-19 TELL US ABOUT THE NATURE OF BIORISKS (WHETHER NATURAL, ACCIDENTAL, OR DELIBERATE IN ORIGIN)?

Natural, accidental or deliberate biological events all fall on the same spectrum of biological risks. Regardless of the source (natural, technological, societal, accidental or deliberate), they all challenge the health systems in similar ways.

In this regard, the COVID-19 pandemic is proving to us that strengthening the international community's preparedness and response to such events is critical even before their origin is completely determined. Therefore, risk-based decision making, risk assessment/mitigation measures, emergency preparedness, response actions and community recovery activities need to be implemented along, *ceteris paribus*, relatively similar models, regardless of the cause.

The COVID-19 pandemic also showcases the centrality of the (public) health sector as a (co)guarantor of countries' security, and the links to animal health issues. Finally, it has shown us that the impact of infectious diseases goes far beyond public health and emergency systems, affecting global socio-economic systems.

If such a disease is deliberately manipulated to be more virulent or is intentionally released in multiple places at once, this could lead to an even greater global crisis.

Therefore, ensuring a comprehensive and holistic approach is pivotal to safeguarding security and guaranteeing safety in all the aspects involving *biorisks*.

IN YOUR OPINION, WHAT IS THE MOST SIGNIFICANT LESSON TO DATE THAT CAN BE DRAWN FROM THE UN RESPONSE TO THE ONGOING CRISIS?

A coordinated and mandate-based approach among and beyond UN agencies to anticipate, assess and mitigate biorisks is critical. Inter-agency cooperation based on trust and understanding of roles and responsibilities as well as capacities and capabilities are key to success in crisis-response, especially during situations characterized by great uncertainty.

Given the interdisciplinary nature of biorisks, which cut across

security, human/animal/plant health, development, humanitarian and other domains, no single organization or expertise can face such events without coordination. When stakeholders from different sectors have to work closely together, a shared understanding and, possibly, the harmonization of procedures, systems, capacities and mechanisms for interoperability becomes essential.

This is true at every stage of an event, for preparedness, prevention, response, mitigation and recovery. Many organizations and nations have acknowledged these challenges and prepared for such contingencies by developing plans and establishing networks.

THE DECISION 2020/59 OF THE SECRETARY GENERAL OF THE UNITED NATIONS ON 20 AUGUST 2020 ESTABLISHED THE UNITED NATIONS BIORISK WORKING GROUP (UN-BRWG). IN YOUR VIEW, WHAT IS THE SIGNIFICANCE/VALUE OF A UN WORKING GROUP TASKED TO ADDRESS BIORISKS COLLECTIVELY?

The UN has processes in place to protect human, animal and plant health and conduct investigations if dangerous biological materials or pathogens are released.

There are three main instruments in place: (i) the 1972 Biological Weapons Convention;

The COVID-19 pandemic is proving to us that strengthening the international community's preparedness and response to such events is critical even before their origin is completely determined

■ © UN Photo/Harandane Dicko

7

(ii) the Secretary-General's Mechanism for Investigation of Alleged Use of Chemical and Biological Weapons; and (iii) Security Council resolution 1540 (2004) regarding the prevention of the proliferation of weapons of mass destruction to non-State actors. Furthermore, the revised International Health Regulations (2005) provide a comprehensive framework for preparedness regarding the public health response to an outbreak of any cause, while the World Organisation for Animal Health (OIE) and the Food and Agriculture Organization (FAO) have similar frameworks in place addressing animal and plant health.

However, the current institutional environment remains fragmented, under-developed and lacking resources, and there are limited processes in place for prevention, prediction and mitigation of biorisks.

In light of this, the United Nations Biorisk Working Group (UN-BRWG) was established to foster coherence and coordination to respond to natural, accidental and deliberate biological events within the UN. Its purpose is not to create a new mechanism/organization but to bring together policy/normative and technical expertise to harmonize and further develop a clear understanding of capacities, mechanisms, and roles and responsibilities within the UN

■ © UN Photo/Harandane Dicko

system in order to strengthen the international community's response to biorisk and improve on the prevention of and preparedness for the deliberate use of biological pathogens.

The UN-BRWG is, therefore, an important step towards defining a common way forward in the field of biorisk. This will contribute to the improvement of health and emergency system capacities as well as interagency interoperability at the national and international levels.

WHAT ACTIVITIES IS THE UN-BRWG UNDERTAKING, AND HOW WILL THESE ACTIVITIES HELP THE UN SYSTEM AND MEMBER STATES BE BETTER PREPARED FOR FUTURE HEALTH EMERGENCIES?

The UN-BRWG is undertaking five activities to enhance interagency coordination and coherence.

In the context of Activity 1, the working group is conducting a mapping exercise of the existing biorisk related roles, responsibilities, expertise and activities within UN entities. This is an essential exercise to iden-

" **The United Nations Biorisk Working Group (UN-BRWG) was established to foster coherence and coordination to respond to natural, accidental and deliberate biological events**

tify the existing resources and possible gaps within the UN system in the area. of biorisk.

In terms of response to a deliberate biological event, Activity 2 is developing the current draft "bio-emergency management framework for deliberate biological events" (being prepared under the Secretary-General's Disarmament Agenda) into an overarching guidance framework for the UN system. The guidance framework aims at fostering UN coherence and coordination to respond to a major disease outbreak of deliberate origin.

Exploring the establishment of a staff exchange programme could be an excellent tool to share knowledge, implement active networks and lay out the foundation for seamless cooperation as well as building expertise and collaboration on biorisk-related topics within the UN. Activity 3 builds on the need to foster interagency collaboration and strengthen internal expertise in order to contribute to a holistic risk management of biorisk related events (especially deliberate).

Activity 4 consists of a high-level UN table-top exercise to test the overarching guidance framework for the UN system developed in the context of Activity 2. The lessons identified from this table-top exercise could be stepping stones towards future exercises focusing on interagency inter-

operability. This exercise will be critical in order to show the relevance of a guidance framework for the UN system for responding to a deliberate biological event.

Finally, Activity 5 aims to develop a UN system strategy and associated implementation plan for greater multi-stakeholder engagement in biorisk mitigation. There is indeed a wide recognition among, inter alia, many States, civil society, researchers, biotechnology companies, and among UN experts that regular and coordinated engagement across the UN system and between stakeholder groups on biorisk related issues would improve preparedness, coordination, cooperation, and response.

These activities are critical as they directly enhance the capability of the UN family to respond to health emergencies in a comprehensive manner and thus to better assist Member States in strengthening their preparedness and response to biorisk related events.

"

The UN-BRWG is, therefore, an important step towards defining a common way forward in the field of biorisk

Sustained investment in prevention and preparedness, as well as enhancing robust global governance to develop predictive mechanisms for coordination are needed in order to realize better preparedness for future health emergencies.

The best defense against disease outbreaks and other health threats is preparedness, which includes investing in building strong health systems and primary healthcare. Health systems and health security are two sides of the same coin. If we don't invest in both, we will face not just health consequences but the social, economic, and political fall-out that we are already experiencing in this pandemic. Additionally, developing robust mechanisms at the global level for assessing multisectoral/ multi-stakeholder preparedness is critical for addressing gaps and advancing coordination for health emergency preparedness and health security. Finally, strong national health systems can help to discourage potential perpetrators from considering the use of biological weapons in the first place, demonstrating the strong linkages between the health and security sectors.

The next pandemic could be more severe than COVID-19. Therefore, we need to leverage lesson-learned and learning from COVID-19 to improve future preparedness, secure the necessary commitments and resources to strengthen our existing tools and capacities, and explore where improvements need to be made.

Dr Michael Ryan, Executive Director, WHO Health Emergencies Programme

Mike Ryan has been at the forefront of managing acute risks to global health for nearly 25 years. He served as Assistant Director-General for Emergency Preparedness and Response in WHO's Health Emergencies Programme from 2017 to 2019.

Dr Ryan first joined WHO in 1996, with the newly established unit to respond to emerging and epidemic disease threats. He has worked in conflict-affected countries and led many responses to high-impact epidemics. He is a founding member of the Global Outbreak Alert and Response Network (GOARN), which has aided the response to hundreds of disease outbreaks around the world. He served as Coordinator of Epidemic Response (2000-2003), Operational Coordinator of WHO's response to the SARS outbreak (2003), and as WHO's Director of Global Alert and Response (2005-2011),

He was a Senior Advisor on Polio Eradication for the Global Polio Eradication Initiative from 2013 to 2017, deploying to countries in the Middle East.

He completed medical training at the National University of Ireland, Galway, a Master's in Public Health at University College Dublin, and specialist training in communicable disease control at the Health Protection Agency in London and the European Programme for Intervention Epidemiology Training.

INTERVIEWED

Izumi Nakamitsu assumed her position as Under-Secretary-General and High Representative for Disarmament Affairs on 1 May 2017. Prior to taking on this post, Ms. Nakamitsu served as Assistant Administrator of the Crisis Response Unit at the United Nations Development Programme (UNDP) since 2014.

She has many years of experience within and outside the United Nations system, most recently as Special Adviser Ad Interim on Follow-up to the Summit on Addressing Large Movements of Refugees and Migrants between 2016 and 2017. She was previously Director of the Asia and the Middle East Division of the United Nations Department of Peacekeeping Operations between 2012 and 2014, and Director of the Department's Division of Policy, Evaluation and Training, from 2008 to 2012.

Between 2005 and 2008, Ms. Nakamitsu was Professor of International Relations at Hitotsubashi University in Tokyo, where she also served as a member of the Foreign Exchange Council to Japan's Foreign Minister, and as a visiting senior adviser on peacebuilding at the Japan International Cooperation Agency. Between 1998 and 2004, she was the Chef de Cabinet and Director of Planning and Coordination at the International Institute for Democracy and Electoral Assistance, based in Stockholm, Sweden.

Earlier in her career, Ms. Nakamitsu was a member of the United Nations Reform Team of former Secretary-General Kofi Annan. She also held positions with the Office of the United Nations High Commissioner for Refugees (UNHCR), including within the office of Assistant High Commissioner for Policy and Operations Sergio Vieira de Mello, and in UNHCR field operations in the former Yugoslavia, Turkey and northern Iraq.

Born in 1963, Ms. Nakamitsu holds a Master of Science degree in Foreign Service from Georgetown University in Washington, D.C., and a Bachelor of Law degree from Waseda University in Tokyo.

INTERVIEWED
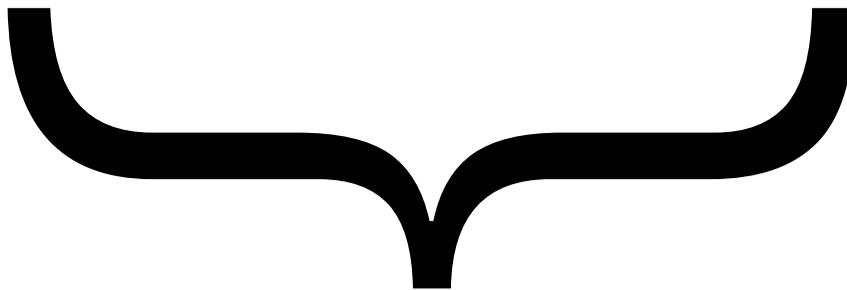
INTERVIEW

INTERVIEW WITH
MS. ANGELICA LIAO-MOROZ

Executive Director, Non-proliferation, Disarmament & Space Division at Global Affairs"; Former Director of Canada's Weapons Threat Reduction Program

by Francesco Miorin

As the Director of the Weapons Threat Reduction Program at Global Affairs Canada since 2018, Ms. Angelica Liao-Moroz has a nuanced understanding of the complexities of national security efforts in an increasingly interconnected global environment. In this interview with F3, Ms. Liao-Moroz shares some of her experience on a wide-range of chemical, biological, radiological and nuclear (CBRN) related issues, from sustainable capacity-building programs to emerging threats.

THE GOVERNMENT OF CANADA IS ONE OF THE KEY DONORS WHEN IT COMES TO INTERNATIONAL ASSISTANCE ON CHEMICAL, BIOLOGICAL, RADIOLOGICAL AND NUCLEAR (CBRN) THREAT REDUCTION, WHAT WOULD YOU SAY ARE THE COUNTRY'S GUIDING PRINCIPLES FOR INTERNATIONAL ASSISTANCE AND COOPERATION?

Canada is proud to be a key player in CBRN threat reduction. But we know we are not alone in this - a threat that affects one can affect us all. No one country or donor can or should go it alone, hence the importance of working in lockstep with the broader international community of governments, experts and organizations. We also very much see it as a full-fledged partnership with those countries or regions seeking assistance, as opposed to a traditional donor-recipient relationship, which makes for greater levels of buy-in and ultimately engagement.

WHY IS CBRN SECURITY ASSISTANCE CONSIDERED A PRIORITY FOR THE GOVERNMENT OF CANADA? HOW HAS THIS CHANGED OVER TIME?

By their very nature, any security incident involving a nuclear, biological or chemical weapon could potentially cripple a city, country or region. A major event could have catastrophic and long-lasting global impacts, but even the improper use of related CBRN materials can pose a risk to communities.

Canada is playing an active role in shaping a range of non-proliferation treaties and initiatives, and is a leading contributor to multilateral groupings. A central one for us is the G7-led Global Partnership Against the Spread of Weapons and Materials of Mass Destruction (launched by Leaders at the 2002 G8 Kananaskis Summit), which as a forum is unmatched in its collective resources, networks and expertise to build capacity to counter such threats.

The Global Partnership itself was a response by the international community to the 9/11 terrorist attacks and the anthrax letter scare in the U.S. This was a major impetus for world leaders deciding to take collective action to prevent terrorists and those that

harbor them from acquiring weapons and materials of mass destruction.

From its beginning, the Global Partnership was primarily focused on helping address the legacy CBRN threats in the territories of the former Soviet Union. There was a significant collective effort focussed on helping Russia destroy its declared stockpile of chemical weapons (the largest in the world at nearly 40,000 metric tons) and the redirection of tens of thousands of former weapon scientists to peaceful pursuits. Things have evolved over time though – today, almost two decades later, the Global Partnership has 31 active members, and has moved beyond the Former Soviet Union (FSU) – the membership delivers programming wherever CBRN threats are present across the globe. It is through the Global Partnership that Canada supports many of the CBRN initiatives in close coordination with our partners.

CAN YOU SHARE A SUCCESS STORY WITH US RELATED TO CANADA'S ENGAGEMENT WITH INTERNATIONAL PARTNERS IN CBRN THREAT REDUCTION?

One success story that I am particularly proud of is all the work we have done to better connect the health and security sectors when it comes to mitigating biological threats - that is to say, the natural, accidental or malicious spread of disease. We are currently assisting more than two dozen countries to strengthen biosafety and biosecurity for pathogens of security concern (e.g. anthrax and Ebola), enhance surveillance and diagnostic capabilities and improve capacities to mitigate all manner of biological threats. We are also spearheading efforts to develop sustainable biosecurity solutions for low-resource countries (including through a "Grand Challenge" to be launched in 2021) as well as a new Global Partnership Signature Initiative to Mitigate Biological Threats in Africa.

Certainly, there's a lot left to do–but we've made significant

strides in the two decades that we've been advocating and steering this collaboration. Through our work on global health security, our program has developed strong ties and partnerships with international organizations such as the World Health Organization (WHO), the World Organization for Animal Health (OIE) and the

supported in the international response to the ongoing COVID-19 pandemic. This includes the biological containment laboratories that we've previously provided to the Caribbean, Ghana, Jordan, Nigeria, and South Africa – these labs are now on the frontlines of testing for COVID-19.

to a quick injection of funding, expertise or equipment. That's probably the exception though – most of our capacity-building efforts require sustained engagement. We are looking to build capacity that will endure well beyond our funding and will have the greatest impact in mitigating CBRN threats.

International Criminal Police Organization (INTERPOL); with other countries and regional partners such as the Association of South East Asian Nations (ASEAN), the Africa Centres for Disease Control and Prevention (Africa CDC), the Caribbean Community (CARICOM) and the Caribbean Public Health Agency). These strong collaborations lead to coordinated programming to ensure that our efforts are targeted and of maximum impact.

We are seeing the impact of many of the initiatives we have

FROM CAPACITY-BUILDING MEASURES TO THE ENVIRONMENT, SUSTAINABILITY HAS BECOME A MAJOR CONCERN FOR DONORS AND INTERNATIONAL ORGANIZATIONS ALIKE. HOW DOES GLOBAL AFFAIRS CANADA APPROACH THIS ISSUE?

Definitely – sustainability is certainly a preoccupation for Canada's Weapons Threat Reduction Program (WTRP). It does come in different flavours or shades though – some of the capacity-building work that we do lends itself

Part of the solution, I think, is to embrace innovation. A great example of this are those biological containment facilities I mentioned earlier. The current "state of the art" in the design and operation of these facilities has been designed for developed countries with ample resources – it is just not feasible to drop them into a lot of these countries where the need is highest. A lot of the most dangerous diseases that we're worried about from a security perspective, such as Ebola or anthrax, are endemic in a number of countries with fairly low levels of infrastructure and resources. So we – by which I mean not just Canada, but other Global Partnership members and international organizations like the WHO and OIE – are working to move away from a "one size fits all" approach and to identify innovative solutions for laboratories to be operated in low-resource environments. For example, we have incorporated solar power into labs we have provided in Nigeria and Sierra Leone. I think we are still in the early stages

17

of this approach though, and we have joined the OIE and the United Kingdom to launch a new "Grand Challenge for Sustainable Laboratories", which aims to develop innovative new technological and operational laboratory solutions that can be sustained in low-resource environments.

ONE OF THE UNITED NATIONS SUSTAINABLE DEVELOPMENT GOALS TARGETS GENDER EQUALITY. WHAT IS GLOBAL AFFAIRS CANADA'S APPROACH TO PROMOTING GENDER EQUALITY THROUGHOUT ITS WORK, ESPECIALLY IN A TRADITIONALLY MALE-DOMINATED AREA SUCH AS THE SECURITY SECTOR? HAVE YOU WITNESSED ANY CHANGE OF DIRECTION IN THIS REGARD?

Meaningful change comes slowly – particularly in a traditionally male-dominated field like the security sector. But make no mistake, we are making inroads. Guided by Canada's Feminist International Assistance Policy, we are applying a feminist lens to all our policies and programming. One way we are doing this is by providing financial support to the IAEA's Marie Sklodowska-Curie Fellowship Programme and to CRDF Global's "WomenAdvance: Chemical Security" program – both aim to increase meaningful participation and create greater opportunities for women in these fields. A lot of the chal-

lenges we see have their roots well beyond the mandate of programs such as ours, and a full solution requires concerted action on a societal level. But I do believe we are helping to move the needle – we are definitely on the right path to promoting women leaders and more diverse voices in this field, which will be stronger for it.

WHAT ARE THE MOST NOTABLE CHALLENGES THAT YOUR ORGANIZATION FACES IN PROVIDING ASSISTANCE?

With finite resources (even for a country like Canada), ensuring that all international assistance is high-impact and value-added is crucial. That being said, we do face a number of challenges when providing assistance to countries. For example, a lot of the peace and security programming that Global Affairs Canada delivers is in countries with multiple and interconnected challenges – economic hardship, impacts of climate change, political instability, and so forth. This means there are often a number of parallel programs and organizations working in the same space, which raises the risk of duplication and the wasting of scarce resources. To help mitigate these risks, we continuously collaborate with our implementation partners, other countries working in the region, and with the beneficiary country

itself to ensure that activities are aligned with development, trade and humanitarian work being conducted.

Additionally, we strive to ensure that any capacity we build in-country related to CBRN threat reduction is sustainable – we have to keep in mind that not all countries have access to the same level of resources. To better ensure the sustainability of our capacity-building projects over the longer term, we work closely on the ground with the stakeholder organizations to make sure they are well-positioned to assume full control and 'ownership' of the project's outcomes (and by 'ownership', I mean more than just a formal handover ceremony and transfer of title – the goal is for the beneficiary to truly step up and assume full responsibility, whether through the ongoing allocation of financial and human resources, or the consistent application of political will).

Lastly, one of the biggest challenges our program faces when providing international assistance is the ability to measure and evaluate results. Our core mandate is to prevent the proliferation of Weapons of Mass Destruction (WMDs) and related materials by terrorists or states of proliferation concern – it is a high-impact but generally low-probability scenario (especially when compared

to the proliferation risks from conventional weapons). It therefore can be difficult to demonstrate value for money and show the public the work we do on the ground to help counter WMD threats. We're working hard with our partners to identify and track relevant performance indicators that will demonstrate an increase in the level of performance by our beneficiaries specifically as it relates to WMDs proliferation, and also as applicable to other global frameworks such as the UN's Sustainable Development Goals (SDGs).

HOW HAS THE COVID-19 PANDEMIC AFFECTED THE WORK OF YOUR ORGANIZATION AND OF YOUR PARTNERS? WHAT LESSONS HAVE YOU LEARNED?

As the events of 2020 have made abundantly clear, an increased focus on strengthening global health security is long overdue. We as societies tend to have fairly short attention spans, and we seem to find ourselves reacting to crises far more than we do working to prevent them. COVID-19 is just the latest example – a virus previously unknown to science has reminded us all that disease can bring the world to a virtual standstill – crippling economies, undermining global security and causing untold human suffering and loss of life. The pandemic has underscored that more collective work is needed to build capacity to prevent, detect and respond to all manner of infectious disease threats, whether natural, accidental or deliberate in origin.

One of the keys to success is collaboration at the health-security interface – that area where the interests of the pubic and animal health communities overlap with those of the international security sector.

19

For the past decade, we have been working with international health partners such as the WHO and OIE to highlight the importance of health-security cooperation, and to build sustainable capacity. This includes support for the WHO to establish a new Health Security Interface Secretariat, and a first-of-its-kind collaboration with OIE, FAO and INTERPOL to build resilience against agro-terrorism and agro-crime by strengthening multi-sectoral capacity and fostering regional and international cooperation.

So there's different stakeholders approaching the same problem but from different perspectives. But ultimately, biological threat reduction and pandemic preparedness require the investment and engagement of a broad group of stakeholders, including from the security sector. And we think this perspective is gradually taking root.

IN YOUR OPINION, WHAT ROLE DOES THE UN PLAY IN PROMOTING CBRN THREAT REDUCTION?

We hear a lot about what an interconnected world we live in, and certainly the pandemic has brought that home! It's undoubtedly true in the world of CBRN as well – a threat that affects one can affect us all. So it's no surprise that the UN is a prime forum to collective-ly address these threats.

For example, UN Security Council Resolution 1540 requires all member states to prevent non-state actors from acquiring, using or trafficking nuclear, chemical and biological weapons and materials. This means that states must adopt and enforce appropriate laws and controls, and report back to the UN on their progress. UNSCR 1540 also helps facilitate assistance to states so they can fulfill their obligations.

In addition, the UN General Assembly offers an inclusive forum to raise awareness and address CBRN threats. Specifically, the First Committee on disarmament and international security adopts a range of resolutions on such threats every year.

OVER THE PAST FEW YEARS, CYBER-ATTACKS AGAINST CBRN FACILITIES HAVE INCREASED SUBSTANTIALLY. CAN YOU TELL US MORE ABOUT GLOBAL AFFAIRS CANADA'S PERSPECTIVES ON THE RISK AND HOW IT COULD BE ADDRESSED THROUGH INTERNATIONAL COOPERATION?

Indeed, malicious cyber activities are increasingly targeting critical infrastructure – we've just seen the news today about a critical oil pipeline in the U.S. being shut down due to a ransomware attack. Canada's Communications Security Establishment's National Cyber Threat Assessment 2020 says that "state-sponsored
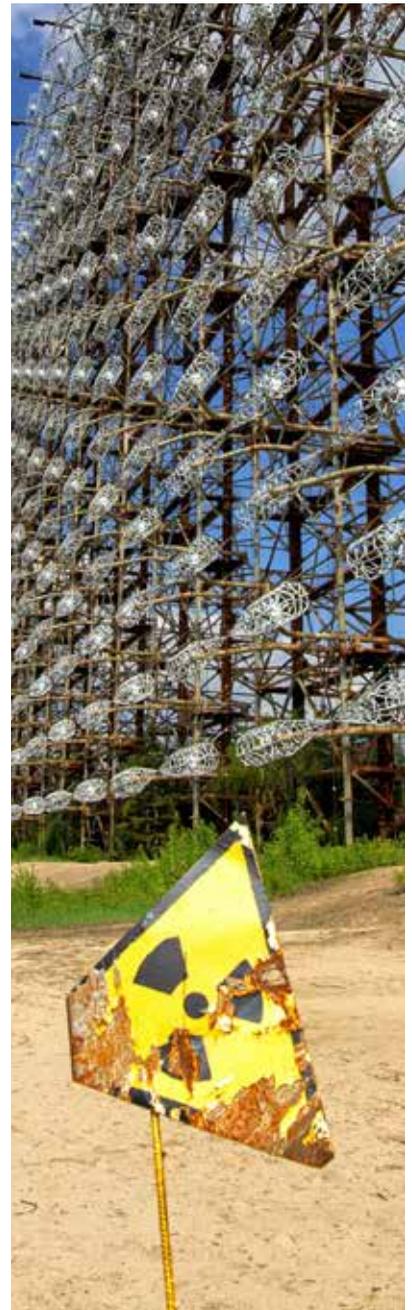
actors are very likely attempting to develop cyber capabilities to disrupt Canadian critical infrastructure, such as the supply of electricity, to further their goals."

It's very much an emerging issue, and I think a lot of us in the international community are

still working to get our hands fully around the challenge. There are already several cyberspace 'norms of state behaviour' endorsed by the UN General Assembly that address malicious cyber activities targeting critical infrastructure. Canada is working with our likeminded partners and allies at the UN and other organizations to promote adherence to a framework of responsible state behaviour in cyberspace. This includes norms of state behaviour and the applicability of international law in cyberspace, as well as calling on all actors not to use cyber means to harm civilians or target critical infrastructure. We're also becoming more fully aware of the need to integrate cybersecurity considerations into our programming activities, particularly for those projects that focus on key infrastructure like nuclear power plants.

WHAT ARE OTHER EMERGING RISKS AND THREATS TO BE ADDRESSED BY THE INTERNATIONAL COMMUNITY IN THE AREA OF CBRN SECURITY?

The introduction of novel technologies present both challenges and opportunities. For example, innovations related to artificial intelligence, 3-D printing, drone technology and advanced nuclear re-

actors can be capitalized for nuclear energy and nuclear applications. However, they can also be double-edged and introduce new threats that could compromise safe and secure operations. Canada is working with partners such as the IAEA, INTERPOL and the World Institute for Nuclear Security to continue addressing these challenges.

There is also the real potential that the misuse of synthetic biology will give rise to new threats – this too requires continued attention. States, through multilateral export control regimes, must also maintain close coordination on safety measures and controls, without unduly stifling legitimate trade.

IF YOU WERE TO CHOOSE ONE, WHAT MESSAGE WOULD YOU LIKE TO PASS TO CANADA'S PARTNERS?

The threat posed by weapons and materials of mass destruction is complex and continues to evolve with the pace of technology, so we cannot be complacent. Collectively, this means we need to be vigilant, adaptable, and get ahead of emerging threats. No one country – however big, active or resourceful – can go it alone.

INTERVIEW

PHOTO GALLERY

The European Union Chemical, Biological, Radiological and Nuclear (CBRN) Risk Mitigation Centres of Excellence (CoE) Initiative (EU CBRN CoE)

4th Preparatory Heads of Secretariats Meeting

9-10 November 2021, Turin, Italy

Since 2018, the Preparatory Meetings have become an important part of the EU CBRN Centres of Excellence, which aims to support Partner Countries and regions in strengthening CBRN risk mitigation and an all-hazards security governance. The format of these meetings is illustrative of the Initiative as a whole: a bottom-up approach in which representatives from the 8 Regional Secretariats showcase their accomplishments and voice their ideas and vision for the way ahead. This year, the vision of Partner Countries was captured in the 2022 Interregional Roadmap that was prepared during the meeting.

- Joseph Maina
  Head of the CBRN CoE Secretariat in Eastern and Central Africa

- Bakhtiyor Gulyamov
  Head of the CBRN CoE Secretariat in Central Asia

- Mari Lursmanashvili
  Head of the CBRN CoE Secretariat in South East and Eastern Europe

- Mohamed Salami
  Head of the CBRN CoE Secretariat in African Atlantic Façade
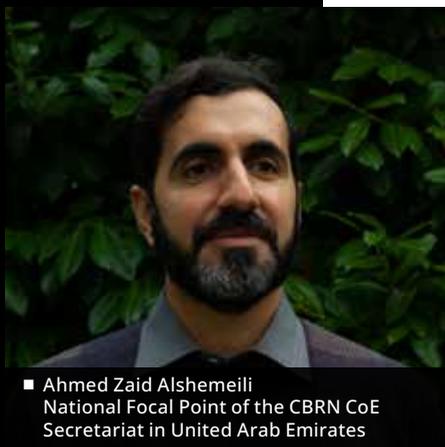
- Ahmed Zaid Alshemeili
  National Focal Point of the CBRN CoE Secretariat in United Arab Emirates

- Ali Cissé
  National Focal Point of Mali, Secretariat of North Africa, and Sahel

During the event, the Kenyan Nuclear Regulatory Authority and UNICRI signed the Memorandum of Understanding for the official inauguration of the Regional Secretariat in Nairobi. The EU CBRN Centres of Excellence now has 8 Regional Secretariats. The other Regional Secretariats are based in: Abu Dhabi, Amman, Algiers, Manila, Rabat, Tashkent and Tbilisi.

Middle East
Amman | Jordan

South East and Eastern Europe
Tbilisi | Georgia

North Africa and Sahel
Algiers | Algeria

Central Asia
Tashkent | Uzbekistan

African Atlantic Façade
Rabat | Morocco

South East Asia
Manila | Philippines

Eastern and Central Africa
Nairobi | Kenya

Gulf Cooperation Council Countries
Abu Dhabi | United Arab Emirates
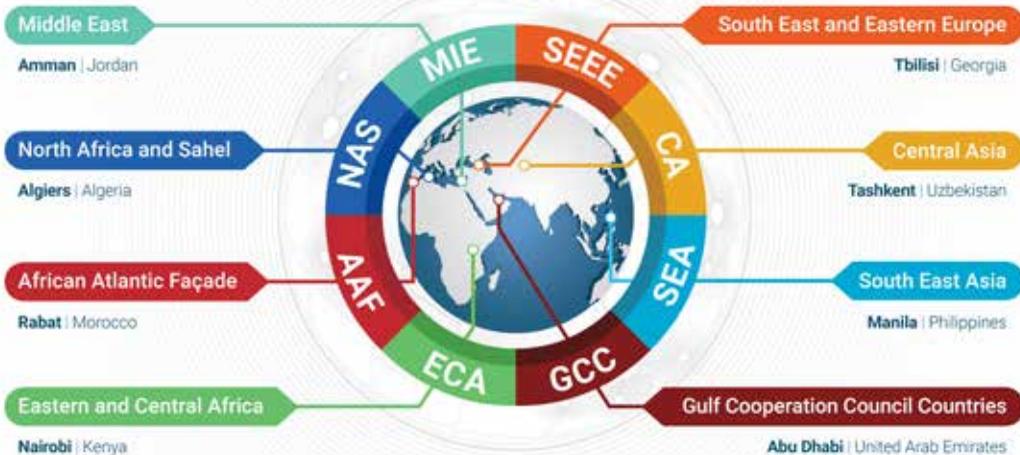
Interregional Roadmap 2022

European Commission FPI Head of Unit, Ms. Natalie Pauwels:
"The Interregional Roadmap is a strategic document that has been elaborated with the participation of all eight regional secretariats. It includes many important objectives to be achieved collectively, in order to maximise the effectiveness of the Centres of Excellence Initiative."

UNICRI Director, Ms. Antonia De Meo: "UNICRI is proud to be part of the EU CBRN Centres of Excellence Initiative since its start, more than 10 years ago, and to work together with key stakeholders and experts in 62 UN Member States every day."

4th Preparatory Heads of Secretariats Meeting

The EU CBRN Centres of Excellence Initiative is implemented through a network, composed of different actors from the Partner Countries, the European Commission and UNICRI. Many of them were present during the meeting.

Heads of Secretariats are designated by the Host Country of the CBRN CoE Regional Secretariat. The Head of the Regional Secretariat guides and promotes the Initiative at the regional level and contributes to the smooth functioning of the Regional Secretariat.

Regional Coordinators are United Nations Officials employed by UNICRI and deployed at the different Regional Secretariats. The Regional Coordinator coordinates the implementation of the CBRN CoE at the regional level, in close cooperation with National Focal Points and the Head of Secretariat.

European Commission

UNICRI supports the implementation of the Initiative, in close cooperation with International Organizations, while the European Commission (EC), in close coordination with the European External Action Service (EEAS) and with technical support from the EC Joint Research Center, oversees overall management. In some EU Delegations, EU Regional Cooperation Officers are also deployed to support the implementation of the Initiative.

National Focal Points (NFPs) are appointed by each Partner Country. Once appointed, the NFP supports the creation of a National CBRN Team, which is composed of representatives from ministries, national agencies and institutions representing relevant communities involved in CBRN risk mitigation.

On-site Technical Assistance (OSA) experts are made available by the European Commission in each region to support project implementers, strengthen cooperation with local authorities, and enhance the technical capacity as well as the visibility of the Initiative.

INTERVIEW WITH THE HEADS OF THE SECRETARIATS OF THE EUROPEAN UNION CHEMICAL, BIOLOGICAL, RADIOLOGICAL AND NUCLEAR RISK MITIGATION INITIATIVE (EU CBRN COE)

by Julie Busch

This article presents the conclusions of the interviews conducted with the Heads of Secretariats of the EU CBRN CoE Initiative.

WHICH ARE THE CRITICAL REGIONAL CAPACITIES NEEDED FOR AN EFFECTIVE RISK CRISIS RESPONSE TO THE COVID-19 PANDEMIC?

The answers of the interviewed Heads of Secretariats focus on three core concepts known as the "3Cs": Coordination, Collaboration and Communication. The 3Cs are considered a pre-condition for an effective response to any CBRN major incident. These three components can be applied for an efficient response to a pandemic such as COVID-19.

Coordination is envisaged at the technical level and focuses on the knowledge of response mechanisms, preparedness with Standard Operative Procedures ("SoPs") and plans of action. These tools should be developed, tested and updated regularly.

Cooperation is intended as interagency cooperation, with the involvement of multiple actors. It must allow to share resources and expertise at national and regional levels. In some regions, the "work in silos" approach adopted by civil agencies has been identified as an obstacle to allow adequate coordination at the national and regional levels. Also, the division between the civil and the military has been pointed as an additional challenge.

Communication is intended as setting clear lines of early communication in order to effectively launch a coordinated response. Yet the COVID-19 pandemic has severely compromised the effective communication of public agencies with the population and challenged the trust in the governments.

WHICH CAPACITIES ARE TO BE CONSIDERED AS STRONG ASSETS IN THE REGIONS?

Good governance was indicated an important capacity present in the regions. This includes, but is not limited to: a clear political engagement to tackle the CBRN risks; the coordination under one authority; a smooth cooperation

between the scientific community and the decision makers and a transparent communication with the public - in particular with young people - based on the good practices observed in neighboring states.

More technical capacities that are present many regions are also considered a great asset, namely: a strong medical infrastructure, well-trained experts in fields linked to CBRN, SoPs already set up to tackle a sanitary crisis (such as Ebola), an adaptable industry in crisis allowing an early production of Personal Protective Equipment ("PPE") and a robust medical surveillance system using artificial intelligence.

IN WHICH WAY HAS THE EU CBRN COE INITIATIVE SUPPORTED THE REGION TO ENHANCE CAPACITIES?

The priorities linked to the COVID-19 crisis response mirror the good practices observed in the different CoE regions: effective communication channels at the regional level; a flexible regional preparedness plan; and the establishment of strong partnerships with the regional industries, policy makers and the scientific community. Raising public awareness on COVID-19 risks and mitigation measures, as well as dispelling misinformation about COV-

ID-19 pandemic and vaccines are also considered priorities.

A wise person once said: "During a crisis, it is too late to exchange business cards." The CoE Initiative has indeed built the infrastructure of interregional communication and cooperation before the onset of the pandemic. In most CoE regions, this allowed for a constant communication amongst National Focal Points throughout 2020 and 2021.

The CBRN CoE also helped build a network of experts from different countries, including the On-Site Assistance experts, who have interacted and exchanged experiences and knowledge based on their respective situations. This resource is considered of tremendous importance.

The Heads of Secretariats indicated several CBRN CoE Projects financed by the European Commission that were particularly helpful in building capacities to deal with the COVID-19 crisis, namely:

▸ Project 53 "Strengthening the national legal framework and provision of specialised training on biosafety and biosecurity" (Central Asia Region).

▸ Project 48 "Improved regional management of outbreaks in the CBRN Cen-

tres of Excellence Partner Countries" (African Atlantic Façade Region).

▸ Project 46 "Enhancement of CBRN capacities in addressing CBRN risk mitigation concerning CBRN first response, biosafety and biosecurity, awareness raising and legal framework" (South East Asia region).

▸ Project 88 "Strengthening of CBRN medical preparedness and response capabilities" (South East and Eastern Europe Region).

▸ Project 34 "Strengthening capacities in CBRN event response and in chemical and medical emergency" (Middle East Region).

▸ Project 33 "Strengthening the national CBRN legal framework and provision of specialized and technical training to enhance CBRN preparedness and response capabilities" (Eastern and Central Africa).

Furthermore, successful projects were implemented in the biorisk area adressing inter-regional needs, namely:

▸ MediPIET "Establishment of a Mediterranean programme for intervention Epidemiology Training" (Project 32).

▸ Stronglabs "Preventing biological risks increased by

environmental and climate change by strengthening public health laboratories" (Project 76).

▶ Medilabsecure "Preventing biological risks increased by environmental and climate change in the Mediterranean, Black Sea and Sahel regions by strengthening institutional capacities in the context of One Health" (Project 75).

▶ Labplus Africa "Strengthening laboratory capacities in Africa against COVID-19 and other epidemics: from set up in Senegal to scale up in Africa" (Project 85).

WHICH ARE THE FUTURE PRIORITIES THAT COULD BE ADDRESSED WITHIN THE FRAMEWORK OF THE EU COE CBRN INITIATIVE?

In the coming years the focus should be on the "lessons learned from COVID-19" in the regions, coupled with an international exercise focusing on a handling the pandemic through cross-border cooperation.

Such exercise would be in line with the past field exercises organized within the framework of the EU CBRN Centres of excellence, in particular the "Jeyran" exercise held in Uzbekistan in November 2019 and the " ARZ exercise" held recently in Lebanon in December 2021.

More generally, biosecurity through a multi-sectoral involvement is of interest in all regions. Capacity building in this area should focus on improving biosecurity management with effective tools to enhance capabilities for highly communicable diseases and global catastrophic biological events, such as pandemics.

Raising awareness of the public as well as improving information sharing and coordination of response plans would be also crucial elements to test.

With special thanks to the Heads of Secretariats of the CoE Intiative:

Ms. Mari Lursmanashvili, Mr. El Hadj Lamine, Mr. Bakhtiyor Gulyamov, Mr. Al Sharif Nasser bin Nasser, Mr. Mohamed Salami, Mr. Camilo Pancratius Cascolan, Mr. Hussein Alharthi and **Mr. Joseph Maina.**

UNICRI
United Nations
Interregional Crime and Justice
Research Institute

AI
ARTIFICIAL INTELLIGENCE
PUBLICATIONS

ALGORITHMS AND TERRORISM:
THE MALICIOUS USE OF ARTIFICIAL
INTELLIGENCE FOR TERRORIST PURPOSES

SCIENCE, TECHNOLOGY AND INNOVATION
UNDERSTANDING ADVANCEMENTS FROM THE
PERSPECTIVE OF
**COUNTERING WEAPONS OF MASS
DESTRUCTION TERRORISM**

**COUNTERING TERRORISM ONLINE
WITH ARTIFICIAL INTELLIGENCE**
AN OVERVIEW FOR LAW ENFORCEMENT AND
COUNTER-TERRORISM AGENCIES IN SOUTH ASIA AND
SOUTH-EAST ASIA

Malicious Uses and Abuses of
Artificial Intelligence

Trend Micro Research
United Nations Interregional Crime and Justice Research Institute (UNICRI)
Europol's European Cybercrime Centre (EC3)

**Download
UNICRI
publications**

ARZ 2021

CHEMICAL, BIOLOGICAL, RADIOLOGICAL AND NUCLEAR EXERCISE ARZ 2021

6-9 DECEMBER 2021

**BEIRUT
LEBANON**

Under the patronage of the President of the Council of Ministers of Lebanon, a 4-day inter-agency Chemical, Biological, Radiologica and Nuclear (CBRN) field exercise "ARZ 2021" took place on 6-9 December 2021 in Beirut, Lebanon.

ARZ 2021, which focuses on countering CBRN terrorism, has been carried out under the leadership of the CBRN

National Coordinator and the European Union Centres of Excellence (EU CBRN CoE) National Focal Point of Lebanon. The event was organized by the United Nations Interregional Crime and Justice Research Institute (UNICRI) in collaboration with the International Science and Technology Center (ISTC), Fondazione SAFE and the on-site assistance expert of the EU CBRN CoE.

The exercise was funded by the Directorate General FPI (Foreign Policy Instrument) of the European Commission within the framework of the EU CBRN CoE Initiative and aimed at testing the capacities of relevant stakeholders and promoting interagency coordination and cooperation to prevent, detect and counter CBRN terrorism at the national level.

The CBRN Counter-Terrorism field Exercise ARZ 2021 was a unique opportunity to address CBRN risks by sharing expertise and improving interagency cooperation. Our deepest gratitude to Lebanon and the other partners of the initiativ

**Leif Villadsen,
Deputy Director of UNICRI**

33

The exercise involved 210 participants, including representatives from different sectors, institutions and agencies, including the Beirut Fire Fighters, the Civil Defence, the Internal Security Forces, the Lebanese Atomic Energy Commission, the, Lebanese Armed Forces and the Red Cross. Each participant played a specific role in the simulation of real incidents, showing the different phases of a terrorism emergency which involve chemical, radiological and nuclear materials.

The two scenarios of the exercise simulated the following situations:

SCENARIO 1:

▶ Illicit hazardous material storage and terrorist laboratory to produce chemical and biological warfare agents, dirty bombs and explosive devices.
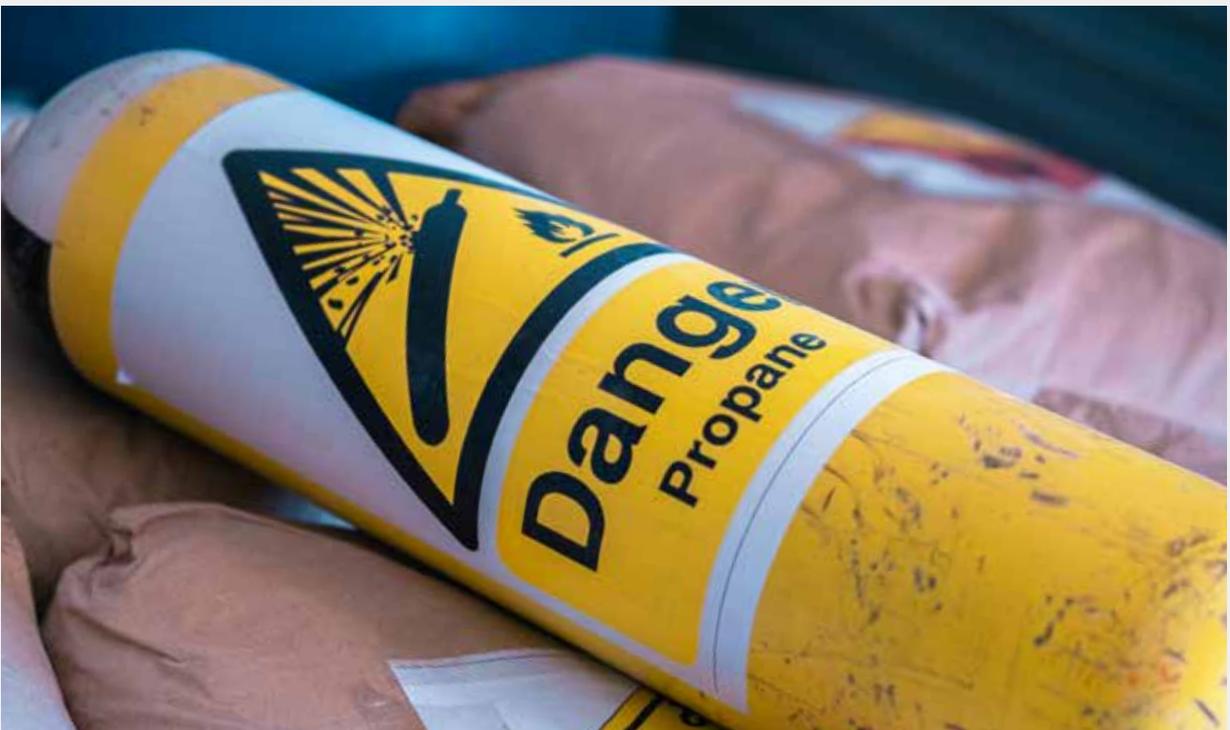
SCENARIO 2:

▶ Attack on a VIP convoy using chemical materials and explosive devices.

The overall development and implementation of the field exercise was evaluated by representatives from the Organisation for the Prohibition of Chemical Weapons (OPCW), INTERPOL, NATO School, the French Police and the Italian Armed Forces.
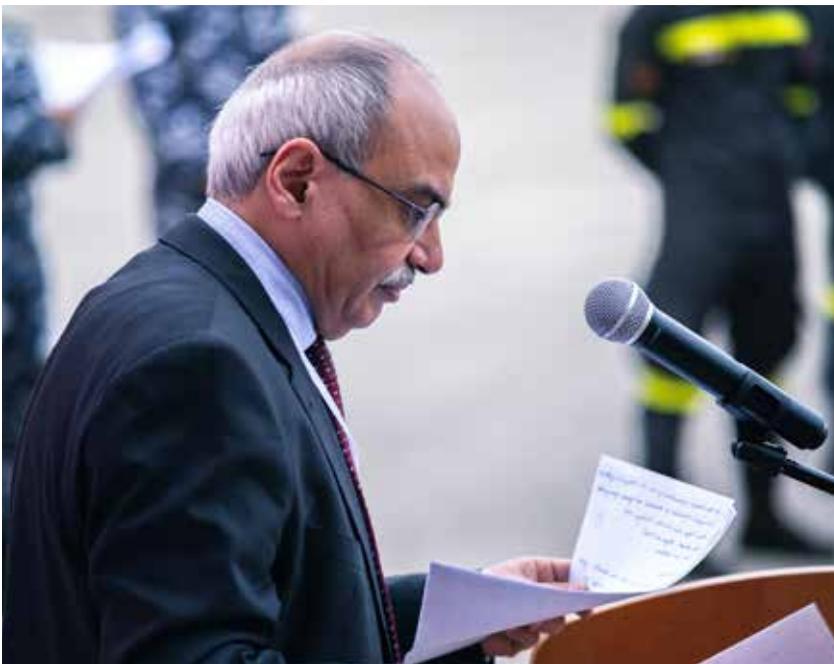
Representatives from international partner organizations and countries attended as observers, namely from the European Union, the European Commission Joint Research Centre (JRC), the CBRN CoE network, Canada, the United States, the League of Arab States and the United Nations Department of Safety and Security (UNDSS).

RESPONDING TO THE THREAT OF TRAFFICKING IN RADIOLOGICAL AND NUCLEAR MATERIAL THROUGH INTELLIGENCE AND LAW ENFORCEMENT OPERATIONS. THE GEORGIAN EXPERIENCE

Interview with Colonel Archil Pavlenishvili, Head of the Operations Division of the Counter-intelligence Department at the State Security Service

by Francesco Miorin

In a wide-ranging interview with UNICRI, Colonel Archil Pavlenishvili, Head of the Operations Division of the Counter-intelligence Department at the State Security Service of Georgia, talks about the importance of intelligence operations to thwart radiological and nuclear (RN) trafficking attempts, the risks connected with RN material falling into the wrong hands, and the challenges faced during his career.

SOMETIMES, WE REGARD THE THREAT OF RADIOACTIVE MATERIAL BEING SMUGGLED AS SOMETHING THAT COULD HAPPEN ONLY IN A JAMES BOND MOVIE. HOW REAL IS THE THREAT? CAN YOU TELL US ABOUT YOUR EXPERIENCE?

Short answer: the threat is real. Here in Georgia, and more generally in former Soviet Union countries, law enforcement organizations are engaged quite frequently in operations to counter smuggling of radiological and nu-

clear material. Just to quote a recent example, just few months ago, my unit successfully carried out an operation and seized a radioactive source which was intended to be smuggled. If we take into account only Georgian statistics, 29 law enforcement operations against smugglers were carried out since 2006, which means that on average one to two operations per year are conducted. Despite the efforts of law enforcement authorities and the high number of arrests,

there still are a lot of attempts to find and then smuggle and sell radioactive sources. Unfortunately, we are forced to spend the majority of our time on scams, on attempts to sell fake radioactive material (such as so-called "Red Mercury") but smuggling of genuine radioactive sources still happens quite often. Other evidence of the reality of the threat is related to the activities of our colleagues from the National Nuclear Regulatory authority: every month they manage to find and seize

66

If we take into account Georgian statistics alone, 29 law enforcement operations against smugglers were carried out since 2006

so-called "orphan sources"[1] in abandoned and active scientific and other civilian installations sometimes even in the field so the threat does exist, and it is quite actual.

WHO ARE THE SMUGGLERS? WHAT ARE THEIR MOTIVATIONS?

That's an interesting question. First of all, when I am talking about smugglers, I am talking about those whom we face in our region (Georgia, Armenia, southern Russia, Ukraine) so it is more or less possible to speak about a "typical" smuggler. The first interesting element is that the majority of the smugglers operating in the region are quite old: the young generations are generally not interesting in buying

"

We have also found "professional criminals", namely professional smugglers who are ready to smuggle any kind of goods, from drugs to weapons and radioactive material

■ Glass jars containing Uranium separated from the ore, also known as "Yellow cake" (Credit: State Security Service of Georgia).

and selling radioactive materials. We refer to them as the "old school smugglers": most of them are in their 60s and sometimes even in their 70s. Normally, they do not have any criminal background: they are either retired scientists or governmental employees from various organizations (mainly civilian), but it happened to us to deal also with retired policemen or retired military officers. Nevertheless, we have also found "professional criminals", namely professional smugglers who are ready to smuggle any kind

of goods, from drugs to weapons and radioactive material.

Most of the "old school" smugglers appear to still live in the post-Soviet early 90s. Back then, the legend of radioactive material being extremely valuable and profitable was born. Most of them believe that even a single successful transaction can make them millionaires. As I said earlier, young people are rarely interested in this. However, in some instances we did face young smugglers, but these are typically the children

■

1   The International Atomic Energy Agency (IAEA) defines an orphan source as "a radioactive source that poses sufficient radiological hazard to warrant regulatory control, but which is not under regulatory control because it has never been so, or because it has been abandoned, lost, misplaced, stolen or otherwise transferred without proper authorization".

■ Criminals often offer fake radioactive material for sale, such as the ones in this picture (Credit: State Security Service of Georgia).

There are connections between organized crime and nuclear and radioactive smugglers

or grandchildren of former smugglers who continue their "family business", if I may call it this way.

When it comes to motivations, the only motivation is virtually always money. Rumors that nuclear energy active sources, even the smallest ones, even the smallest quantities are very expensive and cost millions are hard to remove from the public imagination.

OFTENTIMES, POLITICAL LEADERS AND INTERNATIONAL ORGANIZATIONS HAVE POINTED AT THE RISK OF NUCLEAR TERRORISM AS ONE OF THE MOST CONCERNING THREATS IN THE INTERNATIONAL AGENDA.

WHAT IS YOUR ASSESSMENT? DO TERRORIST GROUPS HAVE THE ABILITY AND WILLINGNESS TO CARRY OUT A TERRORIST ATTACK WITH RADIOACTIVE MATERIAL?

The question of the relation between nuclear smuggling and terrorism is a very important and interesting one, but what I can tell you based on my unit's experience is that we have never faced real attempts from extremists or terrorist groups to obtain radioactive material.

Typically, here in Georgia we face mainly so-called "middlemen": for example, a Georgian criminal is going to sell

radioactive material, but the potential buyer is not the final end-user. Generally, those middlemen are citizens of foreign countries (especially southern neighbors) and they always claim that they are not the final recipients: they either represent someone else or they are going to sell the material in a third country. In light of this, it is difficult to claim that there are no attempts made by terrorist organizations to get their hands on radioactive material. So far, no terrorist or extremist group tried to sell radioactive sources in our territory, we mostly deal with independent individuals, but of course I would not rule out this possibility. Theoretically, it is possible, but in my opinion the main threat is self-radicalized individuals rather than structured terrorist organizations.

These "lone wolves" may believe that they belong to a certain terrorist network, but in fact they are not directly connected with an organization.

43

Nevertheless, they are potential terrorists. For them, an attack with radioactive material may sound attractive. This is why preventing nuclear and radiological smuggling is very important from our perspective.

YOU SPOKE ABOUT THE LINK BETWEEN TERRORIST ORGANIZATIONS AND RADIOLOGICAL AND NUCLEAR SMUGGLERS. WHAT ABOUT ORGANIZED CRIME? HAVE YOU RECORDED ANY INTEREST BY ORGANIZED CRIMINAL GROUPS IN THIS BUSINESS, OR IS THIS MORE RELATED TO INDIVIDUALS AND SMALL GROUPS?

We mainly deal with small groups or sometimes even individuals, although we have had cases involving more complex criminal networks. A few years ago, an organized criminal group led by Valmer Butba in Russian-occupied Abkhazia obtained no less than 10 containers with Cesium-137 sources and tried to sell them. They had found the radioactive material in a coal mine and they were interested in this business though later they abandoned their plans because all their attempts were prevented by our Service.

In our most recent operation, in 2021, we arrested two smugglers who were connected with Georgian criminal authorities living in Turkey, in "exile" let's say. Those professional criminals were super-

vising the activities of the smugglers and had agreed on a percentage from the successful transaction. So, definitely there are connections between organized crime and nuclear and radioactive smugglers.

WHAT IS THE ROLE PLAYED BY INTELLIGENCE AND LAW ENFORCEMENT AUTHORITIES IN COUNTERING THIS PHENOMENON?

You may think I am biased, since I represent a law enforcement organization, but believe me, my words are not an exaggeration. I do not want to over-empha-

size the importance of our work, but the reality is that out of the 29 cases I mentioned, all 29 successful seizures were intelligence-driven, so all of them were full-scale law enforcement operations with the involvement of confidential informants, undercover officers, as well as technical intelligence and other sources of information. I can hardly think of any other tool that is as successful as good intelligence. Of course, there is the so-called "Second line of defense" as our U.S. colleagues call it, namely radiation detection equipment installed at borders and mobile detection equipment, but it is not always effective because you cannot install these devices

■ A typical container for highly-radioactive Cesium-137, referred to as "piglet" in smugglers' jargon (Credit: State Security Service of Georgia).

"Without good intelligence and law enforcement operations it is absolutely impossible to prevent such type of crimes

From a law enforcement perspective I can tell you that the majority of successful operations are based on human intelligence"

45

everywhere and whenever you want. Smugglers have become familiar with these detectors, the locations where they are installed and all the different roads between the countries. In the case of Georgia, we have the additional problem of Russian-occupied territories[2] where there are no State borders at all. So, without good intelligence and law enforcement operations it is absolutely impossible to prevent such type of crimes to and from those territories.

OVER THE PAST YEARS, IT HAS BEEN STRESSED THAT TECHNOLOGICAL DEVELOPMENTS HAVE HAD AN IMPORTANT IMPACT ON THE WAY INTELLIGENCE INFORMATION IS GATHERED AND ON HOW LAW ENFORCEMENT OPERATIONS ARE CARRIED OUT. IS THE MORE TRADITIONAL TYPE OF INTELLIGENCE, THE SO-CALLED "HUMAN INTELLIGENCE", STILL RELEVANT NOWADAYS, WHEN IT COMES TO COUNTERING RADIOLOGICAL AND NUCLEAR SMUGGLING?

It definitely is and it will be. Of course, we live in the 21st century and this is the century of technologies, but from a law enforcement perspective I can tell you that the majority of successful operations are based on human intelligence. Technical intelligence is very important, but it is more of an auxiliary tool in our job. Smugglers are smart enough: they know about the capabilities of special services and police forces to intercept phone calls, break the emails and so on. They do not completely trust their communication systems. The typical conversation between smuggler A and smuggler B is as follows: "Hey, how are you? let's meet and at our place, we need to discuss something", that is it. What can you infer from this sentence? Maybe this is important just to know that some person A is connected with person B, but what are they talking about? Without human intelligence, it is impossible to find out. Out of the famous 29 seizures, only in two cases we relied only on technical intelligence. All the other cases are the result of operations in which confidential informants or undercover officers were involved.

HOW IMPORTANT IS TO COOPERATE REGIONALLY AND INTERNATIONALLY ON RN TRAFFICKING INVESTIGATIONS? WHAT ARE THE OBSTACLES IN THIS REGARD?

As to the first part of the question, the answer is: it is definitely important. An example: as I mentioned earlier, here in Georgia we deal mostly with middlemen. It could be a good idea to give them the chance of smuggling the material to track all the chain (technically, we call these operations "controlled delivery"). It is also very important to identify possible smugglers and possible middlemen in the neighboring countries. But this is the theory: sometimes, the practice is that the relations with some neighboring countries are far from ideal. The first type of challenge is related to the geopolitical situation of the country: it is extremely difficult, if not impossible, to set up an effective system of information sharing with countries that do not have good and stable political relationships.

Bureaucracy and complexity of information-sharing mechanisms are major challenges: the process of obtaining required approvals for sharing information often results in delays which may render the information obsolete. We have to understand that information associated with radioactive smuggling does not belong to police but is considered "national security-level information": limitations are therefore quite strict. Unfortunately, one cannot just simply pick up the phone and call their counterparts in a neighboring country and tell them "Hey, a smuggler is going to travel from our

---

2   The breakaway regions of Abkhazia and South Ossetia.

country to your country and he is looking for radioactive material". Notwithstanding these obstacles, we have managed to successfully carry out cross-border joint operations with some neighboring countries, where our operatives actively cooperated to seize radioactive material and arrest the smugglers.

WHAT ARE THE MOST CHALLENGING FACTORS WHEN DEALING WITH RADIOLOGICAL AND NUCLEAR SMUGGLING?

There are a number of challenges, and most of them are not specific to countering nuclear trafficking but are common to virtually all areas of operation of an intelligence or law enforcement agency. The first challenge I would mention is funding: funds are never enough, and we always need more to effectively perform our functions. Another important challenge is related to Georgia's specific situation with its breakaway regions, and the absence of State borders and detection capabilities, which makes these territories a safe haven for smugglers. In addition to this, high turnover of staff, especially in border police forces represents an issue: trained personnel who underwent training on radiation detection equipment very often move to other positions where salaries are higher or

there are more chances for promotion.

Another challenge we are still facing is the lack of coordination between different State agencies involved in countering RN trafficking: in the past this was a major challenge here, nowadays the situation has improved substantially because all the main actors now know each other personally and there are much fewer issues.

HOW CAN INTERNATIONAL ORGANIZATIONS ASSIST STATES IN TACKLING THIS ISSUE?

International organizations and partners, such as the International Atomic Energy Agency (IAEA), Interpol and UNICRI, as well as partner countries, have helped us a lot in establishing our counter RN trafficking system and in providing radiation detection equipment. What I see as very important is to reinforce training capabilities which many Member States lack: although we do have some training facilities in Georgia, a sustainable and effective training system needs to be put in place, especially considering the high turnover in many State agencies and ministries.

About the Cooperation between Georgia and UNICRI

In 2019, UNICRI launched the CONTACT initiative, thanks to

the generous financial contributions of the Governments of Canada, Norway, United Kingdom and United States of America. The CONTACT initiative is aimed at enhancing capacities of State security, law enforcement and nuclear regulatory authorities of Member States to devise, plan and carry out intelligence and law enforcement operations aimed at thwarting radiological and nuclear trafficking attempts. The initiative is currently being implemented in selected countries in the Middle East, Black Sea region and Southeast Asia.

After graduating from Georgian Technical University in 2006, Colonel Archil Pavlenishvili joined the Georgian Ministry of State Security (MSS, later SSSG - State Security Service of Georgia). He served in counter-terrorism, special operations and counterintelligence units. Since 2005, he heads the specialized counter nuclear/radioactive smuggling unit at the SSSG. A. Pavlenishvili graduated from the George C. Marshall European school for Security Studies (CTC and WMD-T classes) in Germany and Undercover Operations Course in Federal Law Enforcement Training Center (FLETC) in the U.S. He holds a Master's degree in chemistry.

INTERVIEW

TOWARDS A SUSTAINABLE CBRN RISK MITIGATION POLICY IN LEBANON: A SUCCESS STORY IN BUILDING AN EFFECTIVE INSTITUTIONAL SETTING

An interview with Dr Bilal Nsouli, CBRN National Coordinator

by Adil Radoini and Kathy Carroll

Ten years ago, before Dr. Bilal Nsouli assumed his post as the first official Chemical, Biological, Radiological and Nuclear (CBRN) National Coordinator for Lebanon and National Focal Point for the European Union (EU) CBRN Centres of Excellence (CoE) Initiative, little existed in terms of CBRN risk mitigation policy in the country. In his own words, "this was the first time we started CBRN response, before this no one knew what CBRN meant."

In 2012, the Lebanese Prime Minister made the decision to formalize the process of becoming part of the EU CoE Initiative through Dr. Bilal's appointment as the National Focal Point. At that time, Dr Bilal was Director of the Lebanese Atomic Energy Commission, an institute work-

ing under the aegis of the National Council of Research. With the Prime Minister's support, Dr. Bilal assembled a National Team, composed of the army, interior security forces, general security, state security, civil defence forces, and of course the Lebanese Atomic Energy Commission (LAEC). The Prime Minister's decision included a provision to allow this structure to be assisted by any ministries if needed. As such Dr. Bilal was able to call upon technical ministers from the Ministries of Foreign Affairs, Health, Environment, Agriculture, Industry, Economy and Industry as well as members of academia from different universities.

In this extensive interview with F3 Magazine, Dr. Bilal recounts t this feat, which was not an easy task. Not only did he have to deal with government agencies that were working in silos, but he also had to contend with issues of information security, whilst simultaneously attempting to attract external donors.

Even with the support of government's formal mandate, it was impressive to see what Dr. Bilal and the CBRN National Team achieved in such a short period of time. Despite the challenges of the last couple of years – including the tragic Port of Beirut explosions in August 2020, which killed more than 200 people and left many more wounded[1] – Lebanon is investing resources and adopting a systematic approach to tackle CBRN risks.

Lebanon has also managed to attract the interest of several external partners, including the European Union, the United Nations, Canada, the United States, France and many other national and international organizations, to build capabilities in the field of CBRN risk mitigation, resulting in an impressive number of projects coordinated by Dr. Bilal and his CBRN National Team.

LET'S START FROM THE BEGINNING. WHAT DID CBRN PREPAREDNESS LOOK LIKE BEFORE THE EU COE INITIATIVE?

"We started the effort to join the European Union Centres of Excellence Initiative for CBRN risk mitigation in late 2010 – before 2010 the only time CBRN was used was within another project with a significantly different context.

In 2008, we had a project with the European Union (EU) – funded by the EU Delegation in Beirut through a financial arrangement with Lebanese Customs – in order to set up a system for combatting trafficking of radiological and nuclear materials. The implementor of this project was the International Atomic Energy Agency – as the nuclear security office at that time – and coordination came from the Programme Management Office of the Presidency of the Council of Ministers.

From this project, we formed a follow-up steering committee. It was composed of the Programme Management Office of the Presidency of the Council of Ministers, the European Union, IAEA and beneficiaries. This project focused on capacity building for combatting the illicit trafficking of radiological and nuclear ma-

---

1   "On the 4th of August 2020, a pair of explosions of a 2,700 tonnes of ammonium nitrate housed at the port of the city of Beirut, the capital of Lebanon, struck the city, killing more than 200 people, wounding more than 6,500 and causing widespread damage". Source: https://www.theguardian.com/world/ng-interactive/2020/nov/12/beirut-blast-a-night-of-horror-captured-by-its-victims

terials. One of the Work Packages of this project was planning the emergency response to potential incidences of seized smuggled radiological or nuclear materials at the Lebanese borders.

We started to discuss this issue only focusing on emergency response. Later on, IAEA and the EU proposed widening the response plan to encompass CBRN response. This was the first time we heard about CBRN in Lebanon. It was in mid-2008."

WHAT WERE THE MAIN CHALLENGES THAT YOU ENCOUNTERED DURING THIS EARLY PHASE OF THE PROJECT?

"From the beginning the security issue was put on the table: it was difficult to divulgate information that was needed for the gap analysis. At that time, we were very transparent, and we discussed the issue with the different directorates that showed some restriction about divulgating different information. We told them clearly, if we wish to knock the socks off potential donors, we need to show them where we are, what we are doing, what our vision is and what we need from them. We need to show them our seriousness and professionalism. If not, you cannot attract donors."

IT IS CERTAINLY IMPRESSIVE THAT YOU AND YOUR TEAM WERE ABLE TO ESTABLISH CBRN GOVERNANCE AND INTERAGENCY COORDINATION SO RAPIDLY IN LEBANON. WHAT DO YOU THINK IS THE SECRET TO THE COUNTRY'S SUCCESS?

"For CBRN risk mitigation, if you appoint a National Focal Point (NFP) from a list of given stakeholders, this NFP cannot put the all the stakeholders around the same table; we need a higher political cover. Th Prime Minister's Office is at the head, and it means, as NFP, I can work under the umbrella of the Prime Minister's Office, I can make the necessary meetings, by inviting whoever is needed. And, you can head a meeting by representing the Prime Minister's Office. If you do not have this capacity, if you are not

really the guide and if you're not strongly supported by the political system. you cannot work properly

For example, I was able to send letters of invitation directly to the different ministries and directorates, without going through another structure. If you are able to do this, it means what you're saying is coming directly from the Prime Minister.

The second key of success? We need to offer the directories and ministries serious projects where they can see the difference before and after. Directories and ministries need to follow up and to be involved in activities and dialogue."

AIDED BY THE EU COE INITIATIVE, LEBANON ESTABLISHED A COMPREHENSIVE CBRN NATIONAL ACTION PLAN (NAP) FOR THE YEARS 2017-2020 THAT INCLUDED PREVENTION, PREPAREDNESS AND RESPONSE TO CBRN RISKS. NOW YOU ARE PLANNING A WORKSHOP TO UPDATE THE NAP NEXT JUNE. CAN YOU GIVE US AN INSIGHT ON HOW THE PRIORITIES OF LEBANON IN TERMS OF CBRN RISK MITIGATION HAVE CHANGED?

"Priorities are something dynamic, it depends on the threat and risk. For example, from the beginning, in 2012-13, our top priority was chemical weapons used by non-state actors (NSAs), because in Syria and our neighbouring countries, there was evidence of this issue. The top priority

was how to protect Lebanon and the Lebanese population from any NSAs coming from Syria to Lebanon.

Now, the priority has changed. After the Port of Beirut explosions, the priority is totally different. Now, the priority is: to know where we have dangerous chemicals of security concern; where we have dual-use chemicals; to revisit the regulations governing the licensing process of different practices related to these materials; and to see how to destroy and neutralise disused and dangerous chemicals. These are the top priorities, it's something huge, and part of the update will be centred on that. From this priority, we can extract a lot of activities."

CAN YOU TELL US MORE ABOUT THE LESSONS LEARNED AND THE ACTIVITIES RELEVANT TO THE CBRN RISK MITIGATION POLICY THAT WERE TRIGGERED BY THE PORT OF BEIRUT EXPLOSIONS?

"First of all, we were surprised by the vulnerability of the system in the Port of Beirut, and we were also surprised by the governance system at the Port. At the Port, we have different directorates who needed to coordinate with each other, and from what we heard after the explosion, it was really surprising.

From our point of view there are two different things: firstly, how do we improve coordi-nation in the CBRN response and, secondly, what do we need to learn? This explosion taught us a strong lesson that we need more coordination between all directorates in Beirut, and this needs to be done through a Memoran-dum of Understanding (MoU).

We also need a new govern-ance vision in the Port of Beirut: this wasn't a case of someone forgetting to send a notification to another. We need to re-evaluate the whole system of port governance to avoid another explosion somewhere in Lebanon. We need to know how differ-ent directorates coordinated with each other.Their manner of coordinating didn't work because this explosion hap-pened, those materials had been stored for years in Bei-rut. This means you have a governance problem."

LOOKING TO THE FUTURE, I WOULD LIKE TO ASK YOUR OPINION REGARDING HYBRID THREATS IN RELATION TO CBRN. WE HAVE SEEN IN THE NEWS THAT CYBER-THREATS ARE ALSO IMPACTING THE CBRN WORLD IN SOME COUNTRIES. WHAT DO YOU THINK ABOUT THIS THREAT FROM THE CBRN RISK MITIGATION PERSPECTIVE?

"Lebanon has made an effort during the past four years in close cooperation with France to establish a National Com-mittee dealing with cyber se-

curity. We have prepared a National Policy and National Action Plan for cyber security for Lebanon, which was endorsed by the Council of Ministers in 2018. This cyber security plan covers chemical industries in Lebanon (as there are no nuclear or sensitive biological facilities in Lebanon).

In the future, cyber security and CBRN will be directly linked through relevant chemical industries and some critical infrastructure dealing with CBRN materials, for example in the storage of radioactive waste, in order to avoid any sabotage or theft of this material by non-state actors.

There is an intersection between CBRN and cyber security, so cyber security needs to take into account the whole spectrum – the financial sector, telecommunications and CBRN."

DR. BBILAL, IF YOU COULD LEAVE US WITH ONE MESSAGE FOR THE INTERNATIONAL COMMUNITY IN TERMS OF CBRN SECURITY, WHAT WOULD IT BE?

"In most countries, CBRN is implemented with the support of donors, not national budgets. I believe that our countries need to be aware of the importance of that issue and we need a part of national budget to be used for strengthening national capabilities, together with cooperation with international donors. My second message? We need to coordinate all national activities. We need to carry out activities within the endorsed National Action Plan, because, if not, we won't be efficient at all – we will duplicate activities and not make use of the existing resources correctly. We need coordination between donors and stakeholders, and to form a multilateral approach to assistance."

Iraq -Dr Riad Al Tamimi

Iyad Qaddoumi (Interpreter Ar-En)
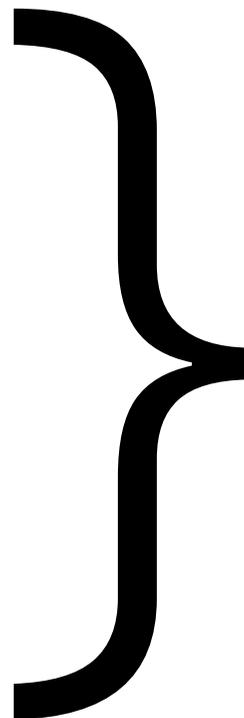
INTERVIEW

CRIME SCENE INVESTIGATION IN A CHEMICAL, BIOLOGICAL, RADIOLOGICAL AND NUCLEAR (CBRN) CONTEXT

by Marián Kolenčík – ISEM Institute[1]

Abstract

CBRN-E crimes are closely linked to environmental crime and their number is constantly growing. Their investigation is a major challenge, and many countries urgently need to improve their systems. An important role for law enforcement agencies is to identify them and provide relevant evidence in court proceedings to ensure that the perpetrators are brought to justice. On-site investigation in the CBRN context must therefore meet high quality standards to maintain the safety of investigators and preserve the evidence. This requires skilled and educated experts.

This article describes the basic attributes of a crime scene investigation under CBRN conditions and recommends a global framework of pro-cedures for investigators, including the use of new technologies. It represents a basis for a future Biological and Chemical Crime Scene Management Guidance Manual for Law Enforcement planned to be developed by an international team of experts under the umbrella of UNICRI.

Introduction

Known assassinations or assassination attempts using novichok, such as the Skripal case in 2018, or the VX case at the Malaysia Airport against Kim Jong-Nam in 2017 or the use of Polonium 210 in the 2006 Litvinenko case, have attracted worldwide attention precisely because of the use of hazardous substances. Other cases that have attracted public attention include the attacks in Tokyo using sarin (1995); letters sent to public authorities in Slovakia con-taining americium 241 (2016); the yperite attack at Tbilisi airport (2018); and the dimeth-ylmercury and abrin case in Czech Republic (2018). Several attempts of terrorist attacks have also been recorded, such as those involving the use of hydrogen sulphide in Australia (2017); ricin in several European countries like Germany (2018); a chlorine bomb (2015) and abrin terrorist plots in Indonesia (2019). All these cases pose a particular challenge for law enforcement agencies and security forces, especially in terms of evidence gathering and quality crime scene processing.

In this context, however, it is also necessary to mention other much more common cases of chemical, biological, radiological, nuclear crimes, even though the definition of CBRN crime is not yet suf-

---

1   First peer review: Cameron Mann (former UK CBRN Police Chief Inspector), Col. Mário Kern (Slovak CBRN Police Chief investigator), Giorgi Beridze (Georgian Forensic Police Expert)

ficiently and uniformly established in the criminal law systems worldwide. These definitions include an increasing trend of assaults using acid; the illegal trafficking, production and possession of CBRN materials; and the illegal transport and dumping of hazardous waste, etc.

We can clearly observe from practice that there is a wide range of CBRN crimes classified under different crime categories. Their impact on the population is often invisible, as it primarily affects the environment and the impact on human health is a secondary consequence. Therefore, it is important to link CBRN crime partially to environmental crime, depending on their type. We can also make this connection on the basis of the existing Directive 2008/99 / EC of the European Parliament and of the Council.[2]

As a good example of combating CBRN/Environmental crimes, we can mention the Slovak Republic, where the police created a special unit within the Criminal Police Bureau focused on combating environmental crime and investigating cases where hazardous materials are involved, unofficially called the Enviro-CBRN Police Unit.

Also, police agencies from the Czech Republic, Georgia and many other countries have a rich experience in dealing with such types of illegal activities. Therefore, it is important to share this knowledge worldwide among law enforcement practitioners, because different CBRN crimes can be interconnected, e.g.: CBRN material illegally dumped in a landfill site can be used for a terrorist attack or for any other offence putting the population in danger.

> **The definition of CBRN crime is not yet sufficiently and uniformly established in the criminal law**

Based on our experience and based on existing international legislation we are preparing a research article about the definition and classification of CBRN crime, which will be published soon. This will address the question of why it is necessary to consider a new, separate and clearly defined category of CBRN crime and will explore the specific methodological, tactical and strategic approach to CBRN crime investigation.

Traditional versus CBRN crime scene investigation

The topic of CBRN crime is complex and is being increasingly discussed worldwide, especially in connection to crime scene investigation (CSI). We often encounter questions as to whether it is necessary to carry out research in this area or to look more deeply at the adequate standard operating procedures necessary to properly secure evidence at the crime scene under hazardous conditions while protecting the health and safety of crime scene investigators.

To this end, it is necessary to compare traditional CSI with CSI in a CBRN context to identify any differences and why it is necessary to specify CSI procedures in a CBRN environment.

As we know from practice, there are different approaches to classical CSI, however each has a common basis and goal. Priority is given to securing the crime scene and evidence, but also to the general protection of crime scene investigators. As stated by the National Forensic Science

2   Directive 2008/99/EC of the European Parliament and of the Council of 19 November 2008 on the protection of the environment through criminal law. https://www.researchgate.net/publication/352860728_CBRN-E_crime_and_offenders'_motives_What_is_it_Why_people_do_it

> **Priority is given to securing the crime scene and evidence, but also to the general protection of crime scene investigators**

■ Czech police via ISEMI

Technology Center,[3] the first is to set the main crime scene dimensions and detect any potential health issue or other hazards. The crime scene must be secured and relevant cordons established. As stated in the United Nations Office on Drugs and Crime (UNODC) Guidebook,[4] one of the main objectives of the protection of the crime scene and its evidence is to ensure appropriate anti-contamination measures in such a way as to protect the integrity of the identified evidence. This objective must be a part of the planning phase.

As stated in another UNODC document written by David James Davis and col.[5] (4), the phases of identification, securing and recovery of evidence from crime scenes represent a challenging part of the investigation. It requires intensive work by investigators and spending the necessary amount of time in performing the duties.

So, what is the difference between traditional CSI and CSI in the CBRN context?

CBRN crime scene investigation is very complex and time consuming compared with traditional CSI. A number of factors play a role that affect the whole chain of custody process. Additionally, compared with a traditional crime scene, the CBRN crime scene contains hazard that could significantly affect the health and safety of investigators and the validity of evidence. A primary CBRN crime scene can be found anywhere: inside an inhabited house, in public buildings and spaces, in industrial enterprises, on critical infrastructure land, on agricultural land, in a forest, in and along a river, in landfills – dump sites, in means of transport, simply everywhere where hazardous materials are commonly present, or where they are transported and used by the perpetrators.

The following four factors must, therefore, be carefully considered in a CBRN context:

■

3   National Forensic Science Technology Center under a cooperative agreement from the Bureau of Justice Assistance, a Simplified Guide to Crime Scene Investigation, USA.
http://www.forensicsciencesimplified.org/csi/CrimeSceneInvestigation.pdf

4   UNODC, Crime Scene and Physical Evidence Awareness for Non-forensic Personnel, New York 2009, ISBN 978-92-1-130273-8.

5   David James Davis and col., Standard Operating Procedure - Crime Investigations in Criminal Justice Compendium for Somaliland, UNODC, 2015
https://www.unodc.org/documents/easternafrica//Criminal%20Justice%20Compendium%20in%20Somaliland/UNODC_ROEA_-_SOP_Crime_Investigations_WEB_LR.pdf

> **The hazardous materials at the crime scene must be accurately detected, identified, monitored and carefully risk-assessed**

I. Specialised equipment and tools

Investigation teams and other cooperating agencies have to be equipped with relevant detection devices and sampling kits for hazardous material or integrated multi-detection systems able to provide reliable data. Simulation and modelling aspects at the contaminated crime scene using new technologies should also be taken into consideration.

The hazardous materials at the crime scene must be accurately detected, identified, monitored and carefully risk-assessed to determine how they should be managed (including the levels of protection required for CSIs).

The transport and deployment of such equipment significantly affects the time and personnel management of activities at the crime scene.

II. Protective requirements

Safety is also emphasized in traditional CSI and priority must be always given to protecting the health and safety of investigators. However, in a CBRN context, the investigators may have to deal with highly hazardous and dangerous materials. This involves the correct selection, dressing and use of personal protective equipment (PPE) that may differ from traditional CSI PPE. When performing on-site tasks, care must be taken to avoid cross-contamination between investigators and to prevent damage to protective clothing. Furthermore, it is important to properly decontaminate, remove and dispose of PPE after completing the work.

In a radiological crime scene, other safety aspects must be considered: time spent in the hazard control area; distance between radioactive sources and CSIs collecting evidence; radiation shielding; the potential spread of radionuclide contamination and monitor-

ing of individual radiation exposure.[6]

The word "contamination" has multiple meanings in CBRN CSI compared to traditional CSI; to prevent the contamination of investigators with dangerous substances; to prevent the contamination of the crime scene and evidence with dangerous substances; and to prevent contamination of other materials that can be transported into a crime scene from outside or from investigators (body fluids, etc.).

It is important to recognise that the work at the CBRN crime scene should only be carried out by police officers or civilians (forensic experts) with specialized training and education. There will always be a limited number of these experts and therefore it is necessary to pay close attention to their protection and safety, as they guarantee the quality of the work.

III. Time and staff resilience

Crime scene investigation in a CBRN context has its specific challenges and requirements, which must be respected early in the planning phase of the activity. In addition to normal police work at the crime scene, it is necessary to take into account the time to put on protective clothing, walk in a CBRN suit to the target place, detect and identify the source of the CBRN threat, its eventual removal, complicated handling of traces in protective suits, decontamination of persons, evidence and used tools. In this connection, there is a limitation resulting from the use of oxygen bottles capacity, radio-communication glitches or the radiation activity of any source present. All these affect not only individual deployment times, but also the number of police officers who have to be deployed to complete tasks. CBRN crime scenes require much more

6   AEA Nuclear Security Series No. 22–G, Implementing Guide, Radiological Crime Scene Management, IAEA, INTERPOL, UNICRI, Vienna 2014, STI/PUB/1672, ISBN: 978–92–0–108714–0, 107.

frequent rotations and replacements of CSIs linked to the level of the hazard and the level of PPE.

IV. Preserving evidence

Detection, identification, collection, decontamination of evidence and packaging of clean, contaminated and decontaminated evidence must be properly performed and recorded to successfully secure and recover them from the crime scene for the chain of custody always bearing in mind the health protection of relevant CSI experts.

Standard operating procedures

The use of the correct methodology and standard operating procedures is therefore of paramount importance in achieving successful prosecutions. Achieving success also depends on multiagency co-

"

Detection, identification, collection, decontamination of evidence and packaging of clean, contaminated and decontaminated evidence must be properly performed and recorded

operation which is not always the case in a traditional CSI. In all phases of the CSI listed below, there must be effective communication and cooperation between several police forces, forensic institutes, firefighters, paramedics and other authorities responsible for CBRN threats like public health authorities, nuclear regulatory bodies, radiological institutes, biological and chemical laboratories, military CBRN protection battalions etc.

Therefore, based on our practical experience we suggest the following necessary procedures for an effective on-site investigation in a CBRN context:

I. Preparatory phase

One of the most important parts of an on-site investigation is proper preparation in the form of obtaining as much information as possible about the case and the environment, i.e. the crime scene. It is essential to collect relevant information from Special Weapons and Tactics (SWAT), Canine (K9) and Explosive Ordnance Disposal

(EOD) teams and non-police agencies like fire fighters, etc. if they have previously intervened at the scene. All collected data will then serve to ensure the safety of CSIs as well as the efficient secur-

ing of evidence. This phase must include the so-called CBRN distance threat recognition (DTR). This is an initial remote detection of CBRN threats through the appropriate standoff detection equipment and visual recognition of CBRN threats remotely (warning signs). Where possible, the investigation team may also use close detection techniques (CDT) in the form of an integrated CBRN threat detection system (UAV - drones and UGV - robots, e.g.: Terrific system and Sense system). Dispersion or contamination modelling and simulation of CBRN threats, together with the modelling of crime scene parameters and characteristics, are strategic tools in this CSI phase. The crime scene security must also be provided by taping the perimeter and marking dangerous zones. Subsequently, crime scene investigators must set priorities for on-site investigation as well as the correct selection and planning of personal protective equipment based on a precise risk assessment. Measures against COVID-19 must also be part of security procedures at the crime scene. Potential contamination of crime scene investigators can endanger their health as well as the health of their colleagues and relatives. For this reason, it is necessary to think about these elements in the preparatory phase.

II. Crime scene reconnaissance

The crimes scene reconnaissance phase follows the previous one, where no weapon or improvised explosive device (IED) threats have been detected by SWAT, K9 and/or EOD teams. It involves the CBRN close threat recognition (CTR) if UAV and UGV couldn't been involved in the previous phase. Subsequently, detailed localization and detection of CBRN and other threats is performed using hand-held detection equipment and visual recognition. Furthermore, all possible obstacles, suspicious objects and substances and potential CBRN booby traps are recorded. This phase also includes an initial inspection of the crime scene, in which all access routes to the primary as well as the secondary crime scene are recorded, if they occur in the common area.

3D Mapping or other commonly used methods may be used to register the crime scene. Finally, criminal investigators record the location, occurrence, and condition of potential traces and evidence.

Accurate photographic and video recordings must be made of this phase, as they will serve for subsequent phases and CBRN profiling of the crime scene and perpetrators. The reconnaissance

■ Slovak police via ISEMI

61

phase is usually carried out in type A protective clothing, unless it is possible to identify the hazardous materials present in advance which allows a risk assessment to determine that a lower level of PPE can be used. Therefore, the default position is type A, which is the highest whole body fully encapsulated protection with independent oxygen flow – self-contained breathing apparatus (SCBA).

As a rule, this part of the crime scene inspection should be carried out, if possible, by the most experienced police officers, as it will result in further action.

III. Planning for sampling, identifying and securing traces and collecting evidence

The next phase is to prepare a plan for collecting samples of CBRN materials and securing identified traces. Planning must include all relevant safety measures as well as a sequence of steps for sampling, securing and collecting evidence. If there are dangerous substances or materials at the crime scene that obstruct investigators from securing evidence, such materials must be safely removed from the crime scene, or neutralized or

shielded - in the case of radioactive sources - by specialised experts.

IV. Sampling, securing traces and collecting evidence at the crime scene

Sampling of suspect substances as well as identifying traces and securing evidence should be carried out in accordance with the established plan.

Samples of hazardous materials taken must be carefully recorded, as well as appropriate measurements by detection instruments. If possible, it is also important to record the GPS locations of evidence and samples, especially if it is an outdoor crime scene.[7]

An inventory log of labelled evidence should be created. The inventory should be carefully double checked for accuracy and all the evidence and samples should be reconciled against the log to ensure they have been correctly packaged and recorded before leaving the crime scene.

Crime scene investigators must be dressed in appropriate protective clothing according to pre-detected threats and a risk assessment, usually level B or C. It may happen in a specific case, that they will

need to wear an A level of PPE at all times.

V. Decontamination of evidence, crime scene and CSI personnel

The decontamination of selected samples of evidence before proper packaging and before transport to the laboratory or police storage room must be carried out in accordance with the relevant standards in such a way that the evidence is not invalidated, compromised, destroyed or rendered unusable. It should be noted that not all secured traces can be decontaminated.

Staff and crime scene decontamination must comply with national and international standards so as not to endanger the health of investigators and others.

VI. Packaging of seized evidence from the crime scene for transportation

Packaging of seized and labelled evidence from the crime scene has to be performed in a way that prevents any cross-contamination. Their transportation must comply with all legal norms to avoid any harm to the environment or health.

■

7   Interpol, Manuel sur les enquêtes scientifiques visant les crimes de pollution, 2015, http://www.interpol.int/Crime-areas/Environmental-crime/Resources or https://docplayer.fr/13414228-Manuel-sur-les-enquetes-scientifiques-visant-les-crimes-de-pollution-volume-ii-de-ii.html

Any evidence or sample transferred from a CBRN crime scene to a laboratory or other suitable evidence storage facility should be accompanied by appropriate records alerting the receiving organisation/staff of any relevant hazards or risks so they can consider how to safely store and manage them.

It is also appropriate to record the various circumstances under which the traces were taken, as this may affect the result of the analysis (e.g. external temperature, contact with other traces, original packaging, etc.).

VII. Profiling - crime scene analysis

Crime scene profiling/analysis in a CBRN context can start directly on-site if a certified profiler/analyst is included in the investigation team or afterwards during the remote desk work using recordings from the crime scene.

In addition to analysis of photographs and video, an integrated approach in assessing the crime scene protocols, investigative, forensic and medicolegal protocols and forensic victimology should be used during the desk work profiling to determine CBRN crime scene characteristics.[8]

If the profiler/analyst takes part in on-site analysis immediately after the crime was committed, they must use appropriate PPE in accordance with the risk assessment.

Further details related to on-site procedures during CSI in a CBRN context, especially in cases of chemical and biological threats, will be elaborated in the framework of the Biological and Chemical Crime Scene Management Guidance Manual for Law Enforcement under the Umbrella of UNICRI's CBRN Programme in cooperation with the ISEM Institute, the EU CBRN CoE, the European Commission, the Biological Weapon Convention Implementation Support Unit and the Organisation for the Prohibition of Chemical Weapons. It will follow the existing International Atomic Energy Agency Radiological Crime Scene Management Guidelines previously mentioned.

THE AUTHOR

Dr. Marian Kolencik, PhD. works as CBRN-E Security Analyst and Profiler specialised in CBRN-E crime and terrorism. His academic background is in the field of Education and Social Science (Slovakia), CBRN Security Management (Poland), Crime Scene Analysis and Criminal profiling (USA). He was also trained in countering CBRN terrorist threats by French police. Since 1995, he has been providing advisory services, training and various analysis for many security forces around the world, and European and international institutions. He is a founder of International Security and Emergency Management Institute - www.isemi.sk

8   Brent, E. Turvey, Criminal Profiling: An Introduction to Behavioral Evidence Analysis, Academic Press, 2011, ISBN 0080569358, 9780080569352, 816 pages,

UNICRI'S EFFORTS IN SUSTAINING THE CHEMICAL AND BIOLOGICAL FORENSIC CAPABILITIES OF ITS MEMBER STATES

by Talgat Toleubayev

Investigation of a crime scene contaminated with chemical, biological or radiological materials poses several challenges to law enforcement authorities in relation to their safe approach and ability to collect and analyze critical evidence, which is vital for a successful prosecution.

The complexity of such scenes requires adequate preparation and planning and the involvement of a wide range of stakeholders, including first responders, specialist police teams, criminal investigators, health and medical experts, staff from laboratories and prosecutors. While many may not be directly associated with the crime scene, understanding the challenges such scenes present will strengthen awareness and interoperability.

> **The complexity of such scenes requires adequate preparation and planning and the involvement of a wide range of stakeholders**

3 CBRN NFP 12 June

While some countries have well developed national Standard Operating Procedures (SOP) and guidelines for Chemical, Biological, Radiological, and Nuclear (CBRN) materials, others have limited guidance or experience in developing such tools. In addition, national procedures are explicitly tailored to a country and therefore, the information it provides is not relevant beyond its geographical boundary. To address this gap, international organizations produce and endorse guidelines developed across the CBRN spectrum applicable transnationally. Some of these guidelines and manuals cater to different aspects of CBRN prevention and response.

The CBRN community acknowledges the need for cooperation between international organizations in developing specific guidance related to CBRN crime scenes.

The CBRN community acknowledges the need for cooperation between international organizations in developing specific guidance related to CBRN crime scenes. The International Atomic Energy Agency (IAEA), was the first to take a step in this direction in 2014

The International Atomic Energy Agency (IAEA), was the first to take a step in this direction in 2014 with the publication of the "Radiological Crime Scene Management Implementing Guide". The Guide was jointly sponsored by IAEA, the United Nations Interregional Crime and Justice Research Institute (UNICRI) and the International Criminal Police Organisation (INTERPOL). The Member States of IAEA widely use its Nuclear Security Series №22G Guidance to comply with their obligations under international legal instruments and conventions. One of the objectives of the IAEA's Implementing Guide is to provide guidance on the investigation of radiologically contaminated crime scenes. Although the IAEA Guide offers a unique support to its end users, its scope is limited to one aspect of CBRN.

To respond to the continued demand for guidance across other aspects of CBRN, UNICRI initiated a new project envisaging the development of the "Chemical and Biological Crime Scene Management Guidebook". The project is funded by the European Commission within the framework of the European Union's CBRN Risk Mitigation Centres of Excellence Initiative (EU CBRN CoE), which celebrated its 10th anniversary in 2020.

The core objective of UNICRI's Guidebook is to provide the target audience and end-users with access to guidance on planning and managing crime scenes contaminated

with chemical or biological agents. To support this objective, UNICRI plans to bring together relevant international organizations and experienced subject matter experts to identify and develop the core themes to assist Member States in processing chemical and biological crime scenes, in a safe and effective way, from the crime scene to the courtroom. The project is divided into phases, each providing a different level of engagement and sustainability.

The Chemical and Biological Crime Scene Management Guidebook will be a high-level strategic document outlining essential content and considerations extrapolated from internationally accepted best practices, examples scenarios and basic crime scene templates relevant to these complex investigations.

In addition to the Guidebook, UNICRI's Chemical and Biological crime scene sustainability package will consist of different phases incorporating the development of chemical and biological crime scene management training curricula,

field exercises, moot court and similar practical scenarios, separately covering chemical and biological crime scene management. These practical elements will be adopted in partner countries based on their needs and inputs and will include strategic tabletop exercises and mock trials, as well as operational exercises.

Both training and field exercises will cover operational and tactical components, complementing the Guidebook's strategic guidance. The Guidebook will focus on interagency and multi-agency coordination and cooperation, by providing insights into the challenges and considerations of chemical and biological crime scene management and prosecution.

The Guidebook aims to adhere to the following characteristics:

▶ Adjustable. The Guidebook provides high-level insights that partner countries can develop and tailor to their existing procedures and/or national legislation and regulation related to the roles and responsibilities of their national CBRN teams, crime

scene processing, and prosecutorial process related to chemical and biological incidents.

▶ User-friendly. The layout and design of the Guidebook will be produced in a user-friendly way, to ensure quick and easy access to core content and references.

▶ Innovative. Using current Quick Response (QR) technology, the Guidebook hopes to include easy access links to downloadable templates for field applications.

▶ Visual. The Guidebook aims to include a number of images and graphics so that end-users can visualize different aspects of the theory.

▶ Multilingual. Initially, the Chemical and Biological Crime Scene Management Guidebook was going to be published only in English. But as project implementation progresses, the hope is to have additional language versions available, by translating the Guidebook into all official languages of the United Nations, and any other languages required.

THE AUTHOR

Talgat Toleubayev is UNICRI's Regional Coordinator within the CBRN Risk Mitigation and Security Governance Programme for South East and Eastern Europe since 2019. He coordinates the activities of 10 countries in the South East and East Europe region within the framework of the European Union's CBRN Risk Mitigation Centres of Excellence Initiative. Prior to assuming this position, he worked at the headquarters of the International Criminal Police Organization (INTERPOL) for more than 16 years.

ATTEMPTS BY NON-STATE ACTORS TO DISRUPT COVID-19 VACCINATION EFFORTS, DELIBERATELY TRANSMIT THE VIRUS AND PROFIT FROM THE SALE OF COUNTERFEIT VACCINES, THERAPEUTICS AND EQUIPMENT

by Francesco Marelli and R. Alexander Hamilton

In the previous article we saw how terrorists and extremists are maliciously using social media to spread disinformation about COVID-19. The present article presents how non-state actors are also seeking to physically sabotage vaccination efforts, deliberately transmit the virus and profit from the sale of counterfeit vaccines, therapeutics and equipment.

Disrupting or sabotaging COVID-19 treatment and vaccination efforts

On 24 March 2020, agents from the United States (U.S.) Federal Bureau of Investigation (FBI) fatally wounded white supremacist Timothy Wilson before he was able to detonate a car bomb outside of a Kansas City-area hospital caring for coronavirus patients. Wilson was active on at least two neo-Nazi Telegram channels and maintained communication with a U.S. Army soldier who expressed interest in attacking a major American news network and targeting a Democratic presidential candidate.[1] Wilson's last online comment was an anti-Semitic message regarding the origin of COVID-19.

More recently, several attempts have been made by non-state actors to sabotage COVID-19 vaccination efforts. On 24 and 25 December 2020, a pharmacist tampered with over 500 doses of Moderna vaccine at Advocate Aurora Health Hospital in the U.S. State of Wisconsin. Facing charges from the Department of Justice, the pharmacist admitted to removing 57 vials of the Moderna vaccine from cold storage at the Hospital, leaving them out to spoil overnight.[2] According to federal prosecutors, the pharmacist held extremist views including that the 9/11 terrorist attacks were faked.[3]

On 18 March 2021, police in the Netherlands arrested a man on suspicion of plotting a crime with "terrorist intent" for allegedly planning to set off a "firework bomb" at a COVID-19 vaccination centre close to Amsterdam.[4]

On 3 April 2021, two Molotov cocktails were thrown at a vaccination centre in Brescia in Northern Italy where COVID-19 vaccines were stored. Although the explosive devices did not cause serious damage, Italy's Carabinieri military police force stated that the arsonists' intention was to sabotage the country's vaccination campaign by

---

1   Levine M. (26 March 2020), 'FBI learned of coronavirus-inspired bomb plotter through radicalized US Army soldier' in ABC News.

2   Ivan Pereira, Alexander Mallin and Sasha Pezenik (27 January 2021), 'Pharmacist pleads guilty to federal charges for intentionally sabotaging COVID vaccines' in ABC News.

3   Todd Richmond (9 February 2021), 'Former Wisconsin pharmacist pleads guilty to vaccine tampering' in Chicago Tribune.

4   The Associated Press (8 April 2021), Dutch police detain man in plot to attack vaccination center.

intimidating the population and fueling a climate of uncertainty. As a result of the investigation, the Carabinieri arrested two members of the "No Vax" anti-vaccination movement. According to the Italian National Associated Press Agency (ANSA), one of the two suspects wrote on Facebook shortly after the arson: "If we want to destroy the enemy we must use the same weapon 'fear' and their fear is our unity."[5]

Each of these episodes demonstrates that the risk of violent non-state actors sabotaging COVID-19 vaccination efforts is a real and on-going challenge, one that is likely to become only more acute as vaccination campaigns gain momentum worldwide.

Deliberate transmission of COVID-19

A second risk concerns the possible deliberate transmission of the SARS-CoV-2 virus. To date, there have been numerous cases in which terrorists and extremists have encouraged their followers to spread the virus to infect opponents. For example, rightwing extremist groups, like CoronaWaffen, have incited followers to spread COVID-19 by "coughing on a local minority" and ISIL has described

> **More recently, several attempts have been made by non-state actors to sabotage COVID-19 vaccination efforts**

COVID-19 as a "divine punishment of arrogance and unbelief." Despite these messages, these groups do not appear to

■ @UN Infodemic

■ @UN Infodemic

5   The Cube (3 May 2021), 'Brescia vaccine centre arson: Italian police arrest two anti-vaxxers for Molotov cocktail attack' in Euronews.

■ © Interpol Terrorism

ca who went to his workplace and a gym while showing COVID-19 symptoms, infecting 22 people.[7]

Sale of counterfeit COVID-19 vaccines, therapeutics and equipment

A third risk concerns attempts by non-state actors to illegally sell or infiltrate legal suppliers with counterfeit or substandard COVID-19 vaccines, medicines or equipment. According to the twenty-seventh report of the United Nations Analytical Support and Sanctions Monitoring Team, established by resolution 1526 (2004), a Member State brought charges against an alleged ISIL facilitator who had operated a website, Face-MaskCenter.com, accused of fraudulently selling personal protective equipment (PPE), including N-95 masks. Another Member State reported that ISIL cells in the Syrian Arab Republic were seeking to profit from the sale of medicines and equipment needed to treat COVID-19 patients.

There have also been examples of criminal groups that have advertised, sold and administered fake vaccines. On 19 November 2020, Gauteng police disrupted an operation selling fake vaccines and

have made serious attempts to weaponize the virus by using contagious supporters to infect opponents.[6]

One recent event, although classified by authorities as a "crime of injury" rather than

an extremist or terrorist act, nonetheless sheds light on the ease with which COVID-19 could be deliberately spread by non-state actors. Specifically, on 21 April 2021, the National Police in Spain arrested a man on the island of Major-

■

6   Twenty-seventh report of the Analytical Support and Sanctions Monitoring Team submitted pursuant to resolution 2368 (2017) concerning ISIL (Da'esh), Al-Qaida and associated individuals and entities, p. 5.

7   Bryan Pietsch (24 April 2021), 'Spanish police arrested a man for spreading the coronavirus to 22 people' in The New York Times.

masks operating out of two warehouses at Growthpoint Industrial Park at Bell Street, Meadowdale, Germiston in South Africa.

On 2 December 2020, the International Criminal Police Organization (INTERPOL) issued an Orange Notice warning of potential criminal activity in relation to the falsification, theft and illegal advertising of COVID-19 and flu vaccines.

Although the non-state actors engaged in these activities would appear to be primarily motivated by profits, rather than a desire to cause deliberate harm, the sale of counterfeit COVID-19 vaccines, therapeutics and equipment could have severe societal consequences. For example, counterfeit vaccines that include toxic ingredients (whether introduced intentionally or unintentionally) could cause significant sickness or death, public alarm and the disruption of government vaccination campaigns.

Francesco Marelli has worked for the United Nations Interregional Crime and Justice Research Institute (UNICRI) since 2003. As the Head of Unit, he is responsible for the coordination of activities in the area of CBRN Risk Mitigation and Security Governance that includes the programme CONTACT to enhance capacities of Member States to prevent the trafficking of radiological and nuclear material, and the implementation of the European Union CBRN Centres of Excellence, a network-based initiative that supports 62 countries to reinforce their national chemical, biological, radiological and nuclear policy.

He is also responsible for the Knowledge Center SIRIO in Geneva that assesses emerging risks and identifies, tests and promotes innovative solutions, including in the area of technology such as Big Data, biotechnology, AI and robotics.

He received a PhD from the School of History of the University of Leeds in 2002. He is author of several publications.

R. Alexander Hamilton has worked with the United Nations Interregional Crime and Justice Research Institute (UNICRI) since 2012, assuming the post of Regional Coordinator for South East Asia in April 2020.

Within the framework of the European Union Chemical, Biological, Radiological and Nuclear (CBRN) Risk Mitigation Centres of Excellence Initiative, his work supports Partner Countries in South East Asia to more effectively prevent, detect and respond to CBRN emergencies, whether natural, accidental or deliberate in origin.

Dr. Hamilton holds a Doctor of Philosophy from the London School of Economics and Political Science (LSE) specializing in risk governance and biosecurity. He has published extensively on these subjects, and is a regular contributor to international efforts dedicated to combating biological weapons.

THE AUTHORS

Social media and messaging apps became a source of collective discussion and response to the coronavirus outbreak

INFOCUS

by Mariana Díaz García

INFODEMIC: RIGHT-WING EXTREMIST GROUPS AND THE RISK OF DISINFORMATION DURING THE COVID-19 PANDEMIC

In December 2019, the Wuhan Municipal Health Commission reported a cluster of cases of pneumonia in the area. By March 2020, the outbreak of the SARS-CoV-2 virus was classified as a pandemic, exponentially increasing the measures that governments took to limit the negative impact on the population, including lockdowns, curfews, and travel restrictions.

All around the world, factors such as home isolation, health concerns about the virus and its socio-political and economic implications generated anxiety and fear. Social media and messaging apps became a source of collective discussion and response to the coronavirus outbreak. Surveys of social media users in different countries have shown an increase in the use of social platforms during the period of physical distancing at home.[1]

In this scenario, right-wing extremist groups have adapted

1   https://www.globalwebindex.com/hubfs/1.%20Coronavirus%20Research%20PDFs/GWI%20coronavirus%20findings%20March%202020%20-%20Multi-Market%20data%20(Release%203).pdf

their propaganda to the online dynamics created by the new extensive online forms of communication consumption generated by the pandemic. These right-wing extremist groups do not represent a coherent movement, yet as defined by the United Nations Counter-Terrorism Committee Executive Directorate (CTED), they are rather a "shifting, complex and overlapping milieu of individuals, groups and movements espousing different but related ideologies, often linked by hatred and racism toward minorities."[2] Other actors, such as organized crime and extremists groups, such as those associated with the Islamic State in Iraq and the Levant and Al-Qaida have also misused social media to pursue their objectives.[3]

The pandemic has created a global unprecedented social media landscape that enabled the spread of conspiracy theories and disinformation. These theories were usually confined by context specific situations in times of crisis. During the global pandemic the impact of these theories have been amplified by the new communication paradigms driven by social media.[4] In this context, extremist groups have found a fertile ground to enhance the impact of conspiracy theories and disinformation to spread their narratives of to restructure their ideology, recruit, and

> " **Right-wing extremist groups have adapted their propaganda to the online dynamics created by the new extensive online forms of communication consumption generated by the pandemic**

---

2   United Nations Counter-Terrorism Committee Executive Directorate (CTED) (April 2020), Trends Alert "Mem- ber States concerned by the growing and increasingly transnational threat of extreme right-wing terror- ism", p. 2. See also the updated version of July 2020.

3   http://www.unicri.it/sites/default/files/2021-01/misuse_sm_0.pdf

4   https://theconversation.com/conspiracy-theories-why-are-they-thriving-in-the-pandemic-153657

incite violent actions during the pandemic. The conspiracy theories attribute the origin of COVID-19 to governments, religious or ethnic groups, secret networks, companies, or businessmen, who in this assumption, are believed to endorse secret agendas such as globalist depopulation, the control of the world or the generation of financial incomes through the sale of vaccines, medical equipment, and drug treatments.

The impact of the fast spread of disinformation was highlighted early by the Director-General of the World Health Organization (WHO) when he expressed that "we're not just fighting an epidemic; we're fighting an infodemic," referring to fake news that "spreads faster and more easily than this virus."[5] COVID-19 conspiracy theories have had several consequences, including jeopardizing the government efforts to implement public health measures and vaccination campaigns, which were observed, for example, in the sabotage of 500 doses of vaccines by a pharmacist in Wisconsin and the infiltration of the far-right extremist groups in the anti-lockdown protests.[6]

The role of technology, particularly social media and messaging apps has been essential for the expansion of malicious activities

"

The role of technology, particularly social media and messaging apps has been essential for the expansion of malicious activities. Right-wing extremist groups have disseminated conspiracy theories by adapting them to their traditional anti-Semitic, xenophobic, and anti-government narratives with the objective of undermining the trust in the government and authorities, reinforcing extremist narratives, improving recruitment strategies, and motivating self-radicalized individuals to perpetrate real attacks.[7] The groups are present on the main global social media platforms.

Some neo-Nazi group groups, have used conspiracy theories to disseminate disinformation and to incite the intentional spread of COVID-19 in Muslim and Jewish communities and have used social media to share hate speech and disinformation, including related to use of vaccines. These strategies adopt some conspiracy theories to engage online users in their ideology and activities. Groups also frequently use memes, videos, animations, and surveys to promote their content.

These activities have generated impact beyond online dynamics. Inspired terrorism was observed when Timothy Wilson plotted to detonate a bomb in a hospital caring for coronavirus patients in Kansas City in 2020.[8] He was active in at least two neo-Nazi social media channels. His last online comment was an anti-Semitic message regarding the origin of COVID-19.

On January 6, 2021, the U.S Capitol was stormed. FBI Director Wray confirmed that advocates of the QAnon conspiracy theory were placed in custody.[9] Jacob Angeli Chansley, "QAnon Shaman", was

---

5   https://www.un.org/en/un-coronavirus-communications-team/un-tackling-'infodemic'-misinformation-and-cybercrime-covid-19

6   https://www.reuters.com/article/us-health-coronavirus-usa-pharmacist/wisconsin-pharmacist-arrested-on-charges-of-sabotaging-covid-vaccine-dos-es-idUSKBN2961YF
     https://riskline.com/party-crashers-the-far-right-at-anti-lockdown-protests/

7   http://www.unicri.it/sites/default/files/2021-01/misuse_sm_0.pdf

8   https://abcnews.go.com/Politics/fbi-learned-coronavirus-inspired-bomb-plotter-radicalized-us/story?id=69818116

9   https://www.dw.com/en/us-qanon-followers-tied-to-capitol-riot-arrested-fbi-says/a-57205833

among the at least 34 QAnon adherents that participated in the siege, while 32 other followers committed ideologically motivated crimes before and after the Capitol insurrection, for a total of 66 who engaged in criminal conduct.[10] Months before the siege, research showed that these groups were motivating their followers to infiltrate anti-lockdown protests and to fabricate homemade weapons to carry them there.[11]

---

10   https://start.umd.edu/publication/qanon-offenders-united-states
11   http://www.unicri.it/sites/default/files/2021-01/misuse_sm_0.pdf

Conspiracy theories and disinformation that are shared by these groups and other actors have other consequences. According to the "Stop AAPI Hate" report, 3,795 anti-Asian racist incidents were reported between March 2020 and February 2021, with 503 incidents in 2021.[12] Furthermore, the convergence of conspiracy theories can have a multiplier effect, reinforcing intergroup polarization and, resulting in jeopardizing government guidance and increasing the risks of terrorist attacks against people or against infrastructures that are connected to COVID-19.[13]

The right-wing extremist groups have tried to use the pandemic to reinforce their narratives, incite potential terrorist attacks, and to recruit new members or increase their followers. The complexity of conspiracy theories, the improvement of diffusion techniques, and the evolution of technology are factors that might increase the threat of disinformation. New social media channels and platforms are also starting to be exploited by these groups.[14]

To fight disinformation, it is important to create counter-narratives and to raise awareness about its consequences, as well as using and developing technology tools and adequate strategies to combat it. Some technology options have been implemented, but the human factor must be included to make a change.[15]
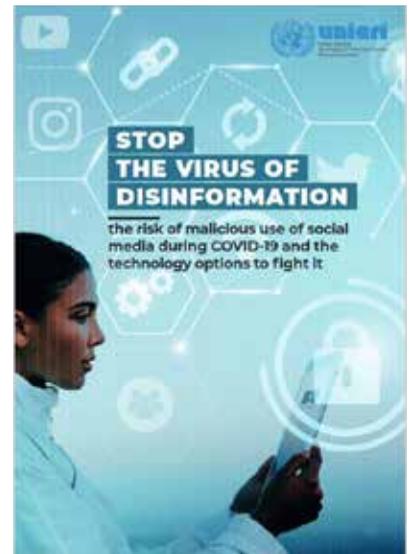
For more information see:
"Stop the virus of disinformation: the malicious use of social media by terrorist, violent extremist and criminal groups during the COVID-19 pandemic."

THE AUTHOR

Mariana Díaz García is currently working as a Fellow in United Nations Interregional Crime and Justice Research Institute (UNICRI) under the framework of the Knowledge Center Security through Research, Technology and Innovation (SIRIO). Her research has focused on the malicious use of social media by extremist groups, technology strategies to improve chemical, biological, radiological and nuclear and Weapons of Mass Destruction (WMD) defense, as well as ideology, radicalization, and legitimization of armed groups.

Ms. Diaz holds a MA in Modern Middle Eastern Studies from Leiden University and a BA in International Relations from Tecnológico de Monterrey.

12 https://secureservercdn.net/104.238.69.231/a1w.90d.myftpupload.com/wp-content/uploads/2021/03/210312-Stop-AAPI-Hate-National-Report-.pdf
13 http://www.unicri.it/sites/default/files/2021-01/misuse_sm_0.pdf
14 https://medium.com/dfrlab/op-ed-the-next-big-wave-of-disinformation-will-be-heard-not-seen-70507fcbf79a
15 http://www.unicri.it/sites/default/files/2021-01/misuse_sm_0.pdf

WOMEN IN CBRN: CHALLENGES AND SUCCESS STORIES FROM THE MIDDLE EAST DURING THE COVID-19 PANDEMIC

Interview with Dr Rana Baydoun - Researcher at the Environmental and Border Radiation Control Department of the Lebanese Atomic Energy Commission (LAEC)

by Heba Mariey

Throughout the past decades, gender-based stereotypes have persisted in the Middle East, posing numerous challenges to women's career prospects and access to many work fields. A career in the field of Chemical, Biological, Radiological and Nuclear (CBRN) security has traditionally been associated with masculinity within the region, offering limited opportunities for women to join and demonstrate their capabilities as security analysts, researchers and officers partaking in the field missions. Moreover, during the past year, the COVID-19 pandemic has further exacerbated gender inequalities in many aspects and presented women with a novel set of challenges that

continue to have a severe toll on their physical and mental wellbeing.

Notwithstanding the challenges, promising examples of Middle Eastern women who have succeeded in breaking the deep-rooted gender stereotypes before and during the pandemic, exist. In a recent interview with UNICRI, Dr. Rana Baydoun, Researcher at the Environmental and Border Radiation Control Department of the Lebanese Atomic Energy Commission (LAEC), briefly discusses her work in the field of CBRN, along with the opportunities and key challenges she has encountered as a female before and amidst the pandemic.

Dr Baydoun,currently in charge of the National Environmental Radiation Monitoring Program, serves as a national trainer for the Lebanese first responder personnel in radiation safety, nuclear security, material out of regulatory control (MORC) and emergency preparedness and response. She is also a quality coordinator at the gamma spectroscopy laboratory. In addition, she has established a Radiocarbon Dating Lab at LAEC, the first of its kind in Lebanon. Besides her vast professional experience for the past two decades, in 2015, Dr Rana concluded her PhD in Environmental Chemistry. She was already well-published before her PhD, and has con-tinued writing papers after it, all while fulfilling her roles as a wife and mother of two.

IN TERMS OF OPPORTUNITIES AND CHALLENGES, HOW WOULDYOU SUMMARIZE YOUR PROFESSIONAL JOURNEY AS A MIDDLE EASTERN WOMAN WORKING IN THE CBRN FIELD?

My passion for science and research has been the catalyst throughout this journey. I first joined LAEC in 1997 as part of a small team responsible for many tasks across different departments. And while this might sound demanding and stressful for many, for me, this was a great opportunity to learn, thrive and progress within the CBRN field. When I started at LAEC I was more focused on the scientific aspects of the radiological and nuclear (RN) fields, but at later stages, I started building up experience in other RN and chemical safety and security aspects, including emergency preparedness and response, radiation safety and MORC.

In terms of challenges, I haven't faced many on the national level. On the contrary, since day one, I have always been supported and guided by my superiors and colleagues at LAEC as well as by my family. Nevertheless, I have experienced moments when I was anxious while assuming certain roles - notably, as a civilian female capacity building trainer for Lebanese military personnel, who were mostly men with middle to high ranks. Relatedly, during these trainings, it has also been challenging to bridge the gap between the scientific and security perspectives of the participants, but together with my colleagues, we have managed to eventually moderate very fruitful and diverse discussions.

On a regional level, unfortunately, as a female, I frequently faced resistance while participating in regional events with other Arab countries, i.e., in the International Atomic Energy Agency (IAEA) technical cooperation events, especially at times when I was the lead counterpart on developing work plans for certain pre-project designs. Making decisions as a female was obviously irritating to many male participants to the extent that they would argue about the validity of the proposals and ideas that I suggested just for the mere fact of me being a woman.

Additionally, the practicalities of conducting field research have sometimes been physically challenging for me as a woman. This included conducting RN research sampling and field surveys, in addition to carrying huge backpacks of portable equipment, if outside LAEC, for very long distances in rough terrain.

https://twitter.com/UNICRI/status/1359925007007244294

https://twitter.com/UNICRI/status/1359925007007244294
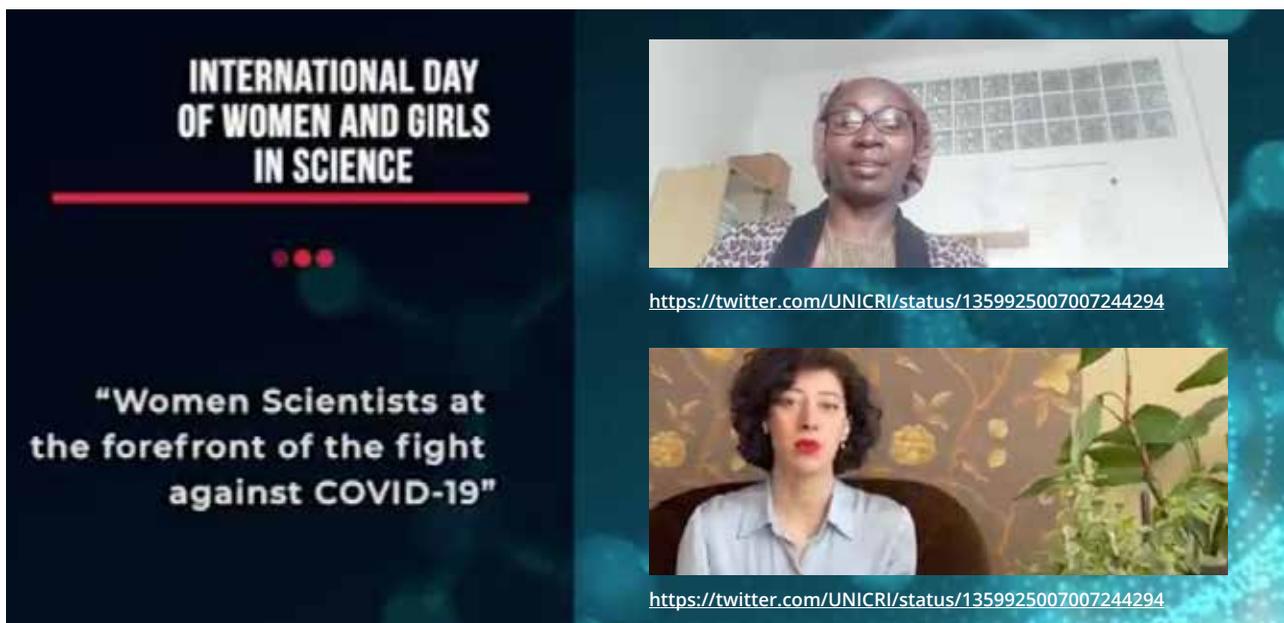
WITH THE OUTBREAK OF THE COVID-19 PANDEMIC AND THE IMPOSED LOCKDOWN MEASURES, HOW HAS YOUR CBRN WORK BEEN IMPACTED?

From an operational perspective, the work of the whole organization has been significantly impacted. National trainings and practical exercises, as well as international cooperation events, have been either halted or conducted online. Unexpectedly, the virtual approach for conducting events has been demonstrably effective in achieving some of the intended outcomes. However, with the practical nature of the CBRN capacity building activities, which should normally include Tabletop Exercises (TTX) and real-life scenarios, adopting the in-person approach is indispensable for ensuring the highest level of effectiveness and interaction. This unfortunately has not been an option so far.

Similarly, with the imposed lockdowns and the strictly designated working hours, the research component has also been severely affected and interrupted. Conducting high-quality scientific research in the applications of nuclear techniques normally requires the availability of certain working conditions, including a convenient, stress-free working environment, concentration, precision, and mind clarity. These have all been so difficult to obtain with the looming stress and anxiety associated with the spread of the COVID-19 virus.

Additionally, there has been a suspension of the national laboratory and equipment installation projects that are conducted within the framework of technical cooperation with the IAEA. The imposed travel restrictions have prevented the IAEA experts from coming over to Lebanon to install the equipment and provide the necessary training for the staff.

DO YOU THINK THAT GOING TO THE OFFICE IN THE MIDDLE OF A PANDEMIC HAS TRIGGERED ANY UNPLEASANT EMOTIONS OF FEAR AND ANXIETY FOR YOURSELF?

Of course. Going to the office has been risky, especially because some of my colleagues tested positive throughout the last year. However, the LAEC was very strict in applying all the necessary precau-

https://twitter.com/UNICRI/status/1359865357553569797

https://twitter.com/UNICRI/status/1359841493893144578

https://twitter.com/UNICRI/status/1359878507933949952

tions at the workplace to prevent the spread of the virus, including wearing face masks and adopting social distancing measures. So, eventually, I haven't experienced so much fear for myself at the workplace, but I have indeed been anxious about transmitting the virus to my family and children. In January 2021, I tested positive for COVID-19 and spread the virus to the rest of my family. However, I didn't catch the virus from my workplace.

WHAT ADDITIONAL CHALLENGES HAVE YOU ENCOUNTERED AS A WORKING FEMALE DURING SUCH AN UNPREDICTABLE TURBULENT PERIOD?

Working from home while setting work-life boundaries and definite working hours has hardly been attainable. Women and mothers are normally expected to shoulder much of the burden at home in contrast with men who can easily manage to isolate themselves at home and set clear, uninterrupted work schedules.

Also, while my husband has been fully supportive during this period, as a wife and a mother, I felt more entitled to address all the lockdown-induced mental and physical distress that my children and husband have been going through.

DO YOU THINK THE PANDEMIC HAS EXACERBATED EXISTING STEREOTYPICAL GENDER NORMS AND ROLES?

Yes indeed. In addition to the inconvenience of working from home for women like myself, whose children are grownups, many other female colleagues with younger children were struggling to balance their work and life roles. With the closure of nurseries and schools during the lockdown, mothers were expected to fulfil their entitled babysitting and care roles, which unfortunately impacted their work and career progress vis-a-vis men.

HAVE YOU FELT SUPPORTED DURING SUCH TIME AT YOUR WORKPLACE? WHAT KIND OF SUPPORT DID YOU RECEIVE?

Of course, my colleagues and I have been constantly supported and encouraged. Most importantly, we have received an abundance of appreciation for efficiently keeping up with the work demands during this unsettling period.

TAKING THE LEAD ON IMPLEMENTING THE CONTACT MIDDLE EAST ACTIVITIES, HOW DO YOU EVALUATE THE WHOLE EXPERIENCE IN TERMS OF OPPORTUNITIES, RISKS, AND CHALLENGES THAT THIS BROUGHT FORWARD?

Honestly, at the very beginning, I was a bit uncertain about the feasibility of implementing the project activities online whilst achieving the intended outcomes. However, the experience of virtually conducting both the Train-The-Trainer session and the National training turned out to be an absolute success. Despite the odds, it presented a unique opportunity for both the trainers and trainees to engage in interactive fruitful discussions and exchange experiences on the topics of preventing the trafficking

of radiological and nuclear material in the Middle East.

The key challenge, I would say, was to ensure that all the COVID-19 necessary precautions were in place to protect the participants.

HOW DO YOU EVALUATE YOUR EXPERIENCE AS A FEMALE TEAM LEADER IN A MALE DOMINATED TEAM OF TRAINERS? DID YOU FACE ANY RESISTANCE OR SPECIFIC CHALLENGES IN THIS REGARD?

Not at all. I decided to present a leadership model that would adopt "teamwork" as an approach to carry out the mission. With this, everyone was encouraged to actively contribute their part to achieve the overall team objectives. Also, as a team, we made sure to provide constant guidance and support to each other throughout the whole coordination and feedback process.

WHAT POLICIES/PRACTICES DO YOU THINK COULD PROMOTE, SUPPORT AND EMPOWER WOMEN WORKING IN THE CBRN FIELD DURING THE PANDEMIC AND BEYOND?

It all starts with the female herself. Breaking the social taboos and advancing women's right to access the security field should evolve from a female's genuine confidence that "she can".

Many women across the region possess the necessary knowledge, skills, and capabilities to pursue their career goals, however without addressing the psychological barriers, including fear and underestimation, other policies will not achieve their intended objectives. I suggest that capacity building is an extremely effective tool in this regard.

The government is also responsible for addressing existing gender inequalities by offering equal opportunities for both women and men to pursue their careers and hold decision making roles within the CBRN field.

INTERVIEW

THE AUTHOR

Rana Baydoun, PhD, is a Researcher at the Environmental Radiation Control Department - Lebanese Atomic Energy Commission, National Council for Scientific Research. She holds a PhD in Environmental Chemistry. She is in charge of the National Environmental Radiation Monitoring Program. She had experience in radionuclide analysis and public dose assessment arising from internal and external exposure. She is Quality Coordinator at the gamma spectroscopy laboratory, and depute of quality manager, and she is experienced in establishing and implementing quality management system according to ISO 17025 standard for calibration and testing laboratories. She is national trainer for first responders. She attended several meetings, conference, workshops and training course in the fields of radiation safety, nuclear security and emergency preparedness and response.

She is involved in the analysis of Materials Out of Regulatory Control, radioisotope identification and activity calculation. Her research interests are in the field of application of nuclear techniques in cultural heritage valorization (Radiocarbon Dating, Thermoluminescence/Optical Simulated Luminescence dating, Uranium/Thorium dating)

Serie of reports about studies on

ILLICIT FINANCIAL FLOWS AND ASSET RECOVERY REPORTS

unicri
United Nations
Interregional Crime and Justice
Research Institute

Download UNICRI publications

INFOCUS

by Katy Carroll

WHAT ROLE DOES LANGUAGE PLAY WHEN REPORTING ON MALE VIOLENCE AGAINST WOMEN?

The tragic murder of Sarah Everard – a 33-year-old marketing executive – in South London on the evening of 3rd March 2021 brought the issue of male violence against women to the forefront of the British national consciousness. As reported in Issue 16 of Freedom From Fear Magazine, the COVID-19 pandemic has seen a rise in violence against women, especially in a domestic setting. This has been seen in countries across the world, including the UK: when looking specifically at the period affected by the coronavirus pandemic, the Office for National Statistics reported that "the police recorded 259,324 offences (excluding fraud) flagged as domestic abuse-related in the period March to June 2020. This represents a 7% increase from 242,413 in the same period in 2019 and an 18% increase from 218,968 in 2018."[1]

---

1   ONS. (2020, November 25). Domestic abuse during the coronavirus (COVID-19) pandemic, England and Wales - Office for National Statistics. https://www.ons.gov.uk/peoplepopulationand-community/crimeandjustice/articles/domesticabuseduringthecoronaviruscovid19pandemiceng-landandwales/november2020

Sarah Everard's murder also sparked a conversation on the language used to report on violence against women in the British media. Although it might not initially seem like the two issues are directly connected, the language that the media uses to report on crime can in fact subtly influence society's cultural mindset and behaviours.

In a blog post for Gender Equal Media Scotland entitled "*How to report sexual assault trials responsibly*" (28th February 2020), Karen Boyle (University of Strathclyde) and Brenna Jessie (Rape Crisis Scotland) explain this link in relation to acts of male sexual violence towards women. They point out that "[t]he audience for sexual assault trial reporting includes potential and actual perpetrators and victim/survivors," and suggest that, "[h]ow these cases are reported can make it more – and less – likely that potential perpetrators reflect on their actions, that incidents are reported to the police, and that victim/survivors seek support."[2]

Boyle and Jessie draw attention to research that has shown the media reporting of court testimony in sexual assault cases rarely accords equal value to the defence and prosecution, saying instead that "it often betrays an implicit bias towards the accuser, his legal team and witnesses by describing their statements in neutral or assertive terms whilst subtly casting doubt on the prosecution."[3]

> **The language that the media uses to report on crime can in fact subtly influence society's cultural mindset and behaviours**

An example of this can be seen in discussions of the evidence and statements given by the defence – that is to say, the legal team and witnesses representing the alleged perpetrator of the crime. When reporting these discussions, the British media tends to use terms such as *said, stated, asserted, denied* – terms that imply fact. In comparison, when reporting on the prosecution and their witnesses – those representing the alleged victim – it is more common for the media to employ vocabulary like *alleged, accused* or *claimed* – terms that could cast doubt on what is being said.

Instead of using terms which could betray bias towards one side of the case, Boyle and Jessie suggest that fair and balanced reporting should use "equivalently weighted terms: she said/ he said; she testified/ he denied."[4]

The blog post is not the first time Boyle has touched on the language used by the media to report on sexual violence against women. In her 2018 article "*Hiding in Plain Sight: Gender, Sexism & Press Coverage of the Jimmy Savile Case*", she discusses the British media´s relationship with TV personality Jimmy Savile, who in 2012 was posthumously investigated for his sexually predatory behaviour. Over the span of his 50-year career, the household name used his position of power to target and sexually abuse large numbers of women and children. However, it was only after his death in 2012 that many of the criminal allegations against him were recognised and investigated.

2   Boyle, K., & Jessie, B. (2020, Feb 28). *How to report sexual assault trials responsibly.* https://www.genderequalmedia.scot/news/blog/how-to-report-sexual-assault-trials-responsibly/

3   Ibid.

4   Ibid.

Boyle analyses the media coverage surrounding Savile's death and concludes that in the early posthumous reports, "his sexual harassment of women is not hidden, but yet cannot be seen as problematic. He is simply a flirt, a womaniser, a ladies' man – all terms which are widely used in the reports following his death."[5] Savile's public persona during his lifetime and immediately after his death was that of a harmless flirt. This persona was created by Savile and made popular by the media.

Boyle's article argues that "one of the reasons Savile's behaviour wasn't recognised and named as abuse in his lifetime – even after the first reports of the allegations which brought about his downfall – is that it was part of a wider cultural acceptance (contemporary as well as historic) of men's sexual entitlement to, and abuse of, women."[6] In other words, Savile's public persona as a harmless flirt meant that those who came forward with allegations of abuse were likely to be dismissed by the establishment. What is more, it is likely that it dissuaded many of his victims from coming forward at all.

It is evident, then, that the language the media employs – and that we also use in our

The language the media employs – and that we also use in our real-life interactions – can have far-reaching implications

"

5   Boyle, K. (2018). *Hiding in plain sight: gender, sexism and press coverage of the Jimmy Savile case.* Journalism Studies, 19(11), 1562-1578. https://doi.org/10.1080/1461670X.2017.1282832

6   Ibid.

> **We must be equally mindful of how we talk about the intersections between areas such as race, class and mental health when reporting on crime**

real-life interactions – can have far-reaching implications. It does not only enable and embolden the perpetrators of violent crimes against women, but also silences the victim-survivors. And, while this article has looked at this question through a gender lens, it is also important to highlight that we must be equally mindful of how we talk about the intersections between areas such as race, class and mental health when reporting on crime.

> **Working to change the public narrative surrounding violence against women and ensure that the stories of victims and survivors are heard**

It should also be noted that there are many journalists and media outlets which are setting the benchmark with regard to responsible and informative reporting. For example, Zero Tolerance, a Scottish charity which work to end violence against women through tackling the root cause of this violence – gender inequality, hold an annual "Write to End Violence Against Women Awards"[7] which champions writers working to change the public narrative

---

7   For more information on the awards: https://www.zerotolerance.org.uk/work-awards/

surrounding violence against women and ensure that the stories of victims and survivors are heard. Zero Tolerance also publish their own best-practice guidelines on the language to be used when reporting on male violence against women.[8]

And, finally, thanks to the democratising influence of social media, we all now have the power to write our own narratives when discussing crime and publicly call out news outlets that use biased or prejudiced language.

THE AUTHOR

Katy Carroll is a linguist from the UK who specialises in Translation and Editing. She currently works in London, translating Life Sciences documents to English. She interned in UNICRI's Public Information Department this year.

---

8   Language guide available from: https://www.zerotolerance.org.uk/language-guide-for-reporting/

HOW CAN NATIONAL AUTHORITIES ENHANCE CBRN HAZARDOUS WASTE MANAGEMENT? – LESS WASTE AND INCREASED AWARENESS

by Dr Yaugen Ryzhykau

First of all, let's unpick the meaning of CBRN security, before considering what could be improved.

In the field of security 'CBRN' is the abbreviation commonly used to describe the malicious use of chemical, biological, radiological and nuclear materials or weapons with the intention to cause significant harm or disruption, as well as technogenic incidents and incidents caused by the delayed on set of hazardous CBRN materials from by-products and wastes. The hazard posed by these materials varies:

▸ **Chemical**
Poisoning or injury may be caused by chemical substances, including traditional (military) chemical warfare agents and harmful industrial or household chemicals.

▸ **Biological**
Illnesses may be caused by the deliberate release of dangerous bacteria or viruses, by biological toxins (e.g. ricin, found in castor oil beans), or by improper management of biomedical wastes.

▸ **Radiological**
Illness can be caused by exposure to harmful radioactive materials or by-products and wastes.

▸ **Nuclear**
Life-threatening health effects can be caused by exposure to harmful radiation, thermal or blast effects arising from a nuclear detonation, or nuclear materials used for peaceful purposes.

CBRN security entails procedures or measures designed to protect the population against the immediate harmful and/or delayed effects of CBRN substances and/or wastes containing such substances, including chemical and biological waste.

Prior even to implementing these "procedures or measures", however, it is crucial that a national strategy for the streamlining of CBRN waste management is developed, required budget allocated and approved by the relevant authorities. By establishing stra-

> **Develop and/ or increase understanding of waste issues in stakeholders/ responsible parties/ policy makers/ technical workers and the public**

tegic targets in the long-recognized hierarchy of waste management, including CBRN hazardous waste, it is possible to attain the ideal outcome, which consists of: prevention, minimization, recycling and reuse, biological treatment, incineration, and landfill disposal of CBRN waste.

In order to achieve the strategic targets, focus should principally be placed on efforts to enhance particular elements of the CBRN material security and waste management capabilities of the respective national institutions. However, complexity arises from the need to follow an identified special approach during the conceptual elaboration of CBRN security strengthening, as well as during the follow-up prioritization of activities on a country-by-country basis, depending on the national CBRN security status at the given time. In order to move towards a "bottom-up approach" – considered being best practice – scientific and technical pragmatic review, as well as consultations and consensus among relevant national and international experts, are crucial elements.

■ ©Steve Watts CBRN Waste
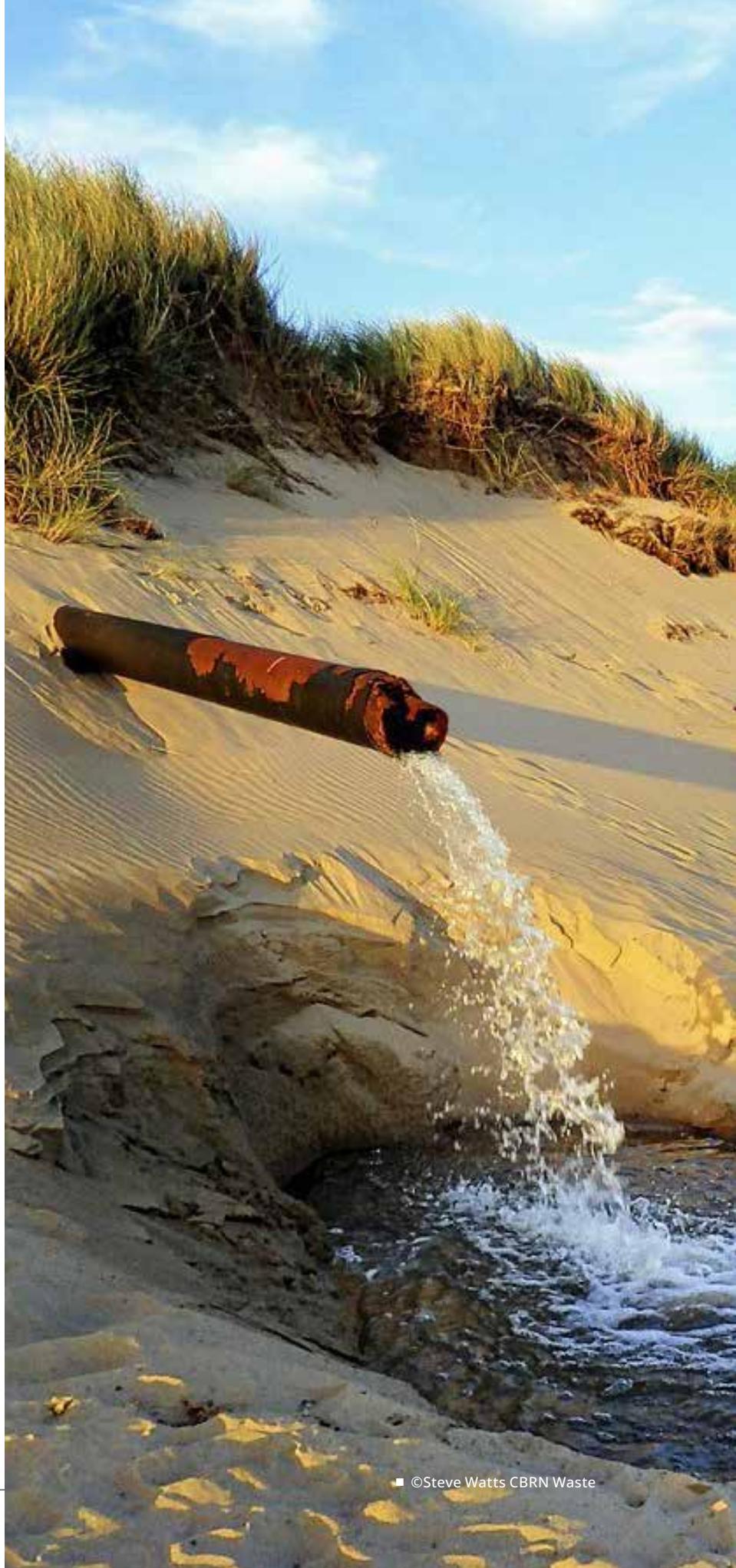
■ ©IAEA CBRN Waste 5

Target groups

The target groups for the implementation of CBRN waste security strategy include, first of all, the legislative and regulatory institutions of the relevant national authority, stakeholders involved in CBRN tasks (such as waste management regulatory authorities, waste management operators, waste transportation facilities, safety and security service providers for the waste management operators etc.),as well as the majority of the population, including the youth.

■ © IAEA CBRN

Overall objective

The overall objective of strengthening hazardous substance waste management for improved CBRN security, including chemical and biological waste, should align with the developed and approved national strategy. It may be achieved through the implementation of the following measures:

▸ **Development and/or improvement of the existent legislative, regulatory and procedural framework,** depending on the current national level. In most developing countries, this is one of the key issues which should be solved first.

▸ **Establishment of a clear and complete structure of waste management bodies, which cover all**

steps of CBRN waste management: safe and secure collection, transportation, separation, processing, storage, disposal and inventory of hazardous CB waste originating from local industry (CBRN waste producers and CBRN waste management facilities), the energy sector, trade, agriculture, health care and past activities (dumping sites, historical industrial sites, former military bases etc.), as well as waste which is a consequence of emergency response and recovery processes.

▸ **Review, find and optimize the necessary resources (financial and material) for the systems and equipment needed by sites/facilities/labs dealing with CBRN waste.** This may include technological equipment for CBRN waste destruction, transportation, packing and storage, supporting materials, PPE and analytical equipment.

▸ **Develop and/or increase understanding of waste issues in stakeholders/responsible parties/policy makers/technical workers and the public,** in order to incrementally raise knowledge to the appropriate level. Knowledge and training should be based on the best practices from developed economies and highly effective, ecologically proven approaches in regard to CBRN waste management.

▸ **Increase number of specifically trained personnel to be able to correctly handle CBRN waste at every step of processing.**

Depending on the country-specific context, the training may start at an introductory level and continue till all personnel are trained adequately.

▸ **Establishing a basic level of and/or improved hazardous waste handling,** including e-waste, plastics and bio medical waste outside of specific sites/facilities, e.g. in household use, municipal waste.

▸ **Review information collected on sites with known chemical and biomedical waste issues and create plans for remediation or clean-up.** Such activities must be conducted under the national relevant legislation and using national and/or international resources.

▸ **Establishment and/or improvement of collaboration between countries in particular regions with regard to joint approaches for CBRN waste management** and response and effects mitigation. Propose, develop and establish a regional, sustainable consultation mechanism that countries may use on a regular and case-by-case basis for CBRN waste issues.

▸ Overall, the implementation of national CBRN waste safety and security – in particular hazardous chemical and biomedical waste management – involves reducing the quantity of hazardous substances produced, treating hazardous wastes to reduce their toxicity, and applying sound engineering controls to reduce or eliminate exposures to these wastes. These measures must be based upon comprehensive national legislation and regulation, the proper education and training of all relevant stakeholders, and the increased awareness of the population as a whole.

THE AUTHOR AND THE PROJECT

Dr Yaugen Ryzhykau, DScTech, qualified Expert for the Secretary-General's Mechanism for Investigation of Alleged Use of Chemical and Biological Weapons (**UNSGM**), is the Project Manager of the European Union Chemical, Biological, Radiological and Nuclear Centres of Excellence Initiative (EU CBRN CoE) Project 65 "Strengthening chemical and biological waste management in Central Asia countries and Mongolia for improved security and safety risk mitigation". He is also Director of the CBRN Protection Training Consulting Technology (TCT) BV. Previously he worked as: Senior Consultant/Special on EC/EU Projects for the Hotzone Solutions Group (HZS); UNOPS Technical Adviser to Libyan National Authorities (NA) for the CWC; Senior Chemical Demilitarisation Officer, Verification Division, Technical Secretariat, Organisation for the Prohibition of Chemical Weapons (OPCW); Head of Scientific and Technical Analytical Centre of NBC troops of Belarus; Senior Researcher and Division Manager of NBC Scientific Research Institute and Testing Ground of the USSR; and member of the investigation mission at Chernobyl accident after-effects.
He is an expert in: WMD and CBRN; CW and CW synthesis and production; CW destruction technologies and toxic waste management; RN safety; Expert in WMD no-proliferation treaties.

About the EU CBRN CoE Project 65 - CABICHEM
The project aims to strengthen existing chemical and biological waste management capabilities to ensure safe and secure collection, transportation, separation, processing, storage, disposal and inventory of hazardous CB waste originated by local industry (CB waste producers and CB waste management facilities), trade, agriculture, health care and past practices (dumping sites, historical industrial sites, former military bases etc.), as well as a consequence of emergency.

CABICHEM is funded by the European Union through its Instrument contributing to Stability and Peace and implemented to benefit the partner countries of the region of Central Asia, namely the Islamic Republic of Afghanistan, the Kyrgyz Republic, Mongolia, the Islamic Republic of Pakistan, the Republic of Tajikistan and the Republic of Uzbekistan.

Project 65 seeks to support national and regional bodies involved in the waste management main issues as well as to assist countries in reviewing and evaluating their legislative provisions on the matter. The project aims further to raise awareness of the issues associated with chemical and biological waste management as well as to provide training activities, including the train-the-trainer approach also based on a tailored e-learning instrument.

The project is coordinated by Military Institute of Chemistry and Radiometry – MICHR from Poland, and will be implemented by Fondazione FORMIT, the Istituto di Scienze e Tecnologie Molecolari – ISTM-CNR from Italy, the Military Institute of Hygiene & Epidemiology – MIHE from Poland, the Fondazione Alessandro Volta – FAV from Italy. Local senior experts with experience in CBRN domain are supporting the activities in the partner countries.

WHY IS CHEMICAL AND BIOLOGICAL WASTE MANAGEMENT RELEVANT TO CHEMICAL, BIOLOGICAL, RADIOLOGICAL, NUCLEAR, AND EXPLOSIVE MATERIAL RISK MANAGEMENT?

The example of Project 67 of the European Union Chemical Biological Radiological and Nuclear Risk Mitigation Centres of Excellence Initiative

by Dr. Hendrik Visser, Sustainable Criminal Justice Solutions Europe

" Strengthening CBRNE risk-mitigating frameworks and infrastructures enhances general waste management systems

O ver the last few decades, awareness about environmental issues has increased significantly among the general population. Including, the understanding by the public of the importance of appropriate waste management, exemplified by the 3 R's concept: Reduce, Reuse and Recycle. However, not everyone is aware of the fact that addressing waste management issues is also essential for the mitigation of risks related to chemical, biological, radiological, nuclear, and explosive (CBRNE) materials. And, vice versa: strengthening CBRNE risk-mitigating frameworks and infrastructures enhances general waste management systems.

Therefore, international and national CBRNE programs and initiatives, such as the European Union Chemical Biological Radiological and Nu-

©Hendrik Visser

clear Risk Mitigation Centres of Excellence Initiative (EU CBRN CoE), have concentrated efforts and resources on hazardous waste management projects. Such projects aim at strengthening and developing the frameworks and infrastructures to manage the risks associated to CBRNE incidents.

Incidents involving hazardous CBRNE contaminants can create significant challenges, such as: minimising the amount of waste generated during clean up and remediation; segregating waste types; packaging and safe transportation of the waste; and treating and disposing of waste and debris. Furthermore, these complexities related to waste management are in some countries compounded by:

▸ Limited disposal and treatment expertise, capabilities and capacity to manage CBRNE contaminated waste.

▸ Lack of experience of decision-makers and absence of waste management facilities to handle these wastes.

▸ Hesitancy on the part of some disposal facilities to accept these wastes.

▸ Limited resources to cover the (at times high) costs of disposing of hazardous waste.

©Hendrik Visser

99

Throughout the incident response and clean-up process, wastes must be characterised to minimise human and environmental exposure to contamination and determine how and where to transport, treat and/or dispose of contaminated materials. Response to a large-scale incident is also difficult because there are often interrelated activities. For example, choosing a decontamination approach has an impact on the timeline of the remediation as well as the cost and the amount of waste generated. Therefore, decision-makers need to be aware of the trade-offs involved in their decisions to optimise the response. In order to enhance the effectiveness of the response, a multi-sectoral stakeholders decision making approach is to be encouraged.

To address these challenges and to manage the risks associated with CBNRE materials, certain frameworks and conditions need to be in place, among others:

▸ Legislative and regulatory framework.

▸ Implementation and enforcement.

▸ Incidence response.

"

Decision-makers need to be aware of the trade-offs involved in their decisions to optimise the response

Legislative and regulatory framework

The foundation for risk management is a clear legal framework at international, national and local levels, which establishes the main rules for safe and secure work with CBRNE materials, including waste. Violations of these rules can entail responsibility, including criminal responsibility by individuals, organisations or states. Without such a framework, it would not be possible to prevent, investigate or prosecute criminal conduct properly.

The foundation for risk management is a clear legal framework at international, national and local levels

"

Although such a legal framework focusses on safe and secure work with hazardous materials, such as production, transport and waste disposal of chemical and/or biological materials. These frameworks also address the response to incidents due to natural disasters, industrial accidents, and criminal/terroristic acts, which are the primary focus of CBRNE programs. Therefore, by strengthening this general legal framework, the specific legislative tools required for CBRN risk management are also reinforced.

Additionally, it is of great importance to have international agreements in place that stimulate harmonised national legislation to prevent geographical loopholes. This is especially true in light of the trade of hazardous materials by multinationals and criminal organisations that operate globally.

Implementation and enforcement

Even if comprehensive, global agreements are in place, it is important to implement and enforce them adequately. In order to do so, governmental structures that have the right to enforce legislation with respect to production, transportation and disposal of chemical and biological materials need to be in place. The staff of these departments and agencies should be trained

appropriately in national and international legal requirements and have sufficient technical understanding of the issues involved. Additionally, technical infrastructures should be established to inspect or investigate, respond to contamination events and, in certain cases, remediate sites, which require capacity (i.e., equipment) and capabilities (trained staff) or the ability to access these.

Moreover, legislative/guidance resources need to be available to companies that work with chemical and biological materials in order to establish their operation within the legal requirements. Examples of such resources could be having access to clear guidelines on how to operate legally; a formal system of registration of their activities (including waste generation); and opportunities to consult with regulatory authorities (including training on requirements).

Many of the technical capacities and capabilities required for chemical and biological waste management are also necessary for CBRN risk management. Therefore, like with the legislative framework, enhancing chemical and biological waste management implementation and enforcement also strengthens CBRN risk management.

Incident response

In case of an industrial accident, criminal disposal, environmental outbreak or terrorist attack involving chemical or biological materials, correct capacities and capabilities need to be in place to deal with such crises. Some of the response capacities and capabilities overlap with those required for waste management implementation and enforcement. However, certain capacities and capabilities are specific to incident responses and require additional equipment and training of personnel dealing with such situations. Most if not all of the capacities and capabilities in incident responses match the ones needed for CBRN risk management.

Moreover, many countries worldwide deal with legacy waste deriving from previous economic or governmental activities. The way they address the issue of legacy waste is similar to incident response, although there are differences between the two cases. For example, if the issue to be addressed involves chemical or biological materials in storage facilities or contaminated sites, the tools first used to identify this type of waste are similar to the investigative tools necessary to control current companies or respond to incidents. Ad-

> **Enhancing chemical and biological waste management implementation and enforcement also strengthens CBRN risk management**

ditionally, the technological solutions for remediation of contaminated sites by legacy waste are similar to those involved in the clean-up after an incident. However, often, the scale of the legacy sites will require either significant governmental or private investment to remediate a site to an acceptable level.

Therefore, in summary, by strengthening chemical and biological waste management, the (legislative) tools and components (infrastructures and human resources) to prevent, respond and mitigate chemical and biological incidents are enhanced as well. It is also imperative to support and stimulate a multi-sectoral stakeholders' coordination and response, as each stakeholder will have different responsibilities, capabilities, capacities that need to be organised appropriately to achieve an effective response.

As stated above, the EU CBRN CoE Initiative is funding multiple projects on CBRN waste management to address some of the challenges and issues mentioned earlier. One example is Project 67 (P67), titled 'Strengthening CBRN Waste Management Capabilities in South-East and Eastern European Countries'. Several areas previously discussed are addressed within the framework of this project, such as:

Supporting the strengthening of legislative frameworks

Legislative assessments were performed, and recommendations formulated for the ten partner countries (Albania, Armenia, Azerbaijan, Bosnia and Herzegovina, Georgia, Moldova, Montenegro, North Macedonia, Serbia and Ukraine) with regards to chemical, biological and radioactive waste management. Several partner countries expressed interest in receiving further support to strengthen their legislative framework and enhance implementation and enforcement.

Strengthening waste management infrastructures

All partner countries were visited, and a list of equipment required for waste management was formulated, with the expectation that some of the costs of the requested items will be covered under the umbrella of a follow-on project. The overall aim of this activity was to identify the areas where the technical capacities of the partners need to be strengthened.

Development of training capabilities

As indicated above, it is essential to provide entities working with hazardous materials resources to understand their legal and technical obligations. One of the means to address this need is by having a cadre of experts in the country that can train stakeholders on the legislative and technical aspects of waste management. Therefore, as part of P67, training-of-trainers workshops are conducted on chemical and biological waste management in order to support partner countries to create a team of trainers that can teach governmental and private stakeholders in chemical and biological waste management issues (legislative issues, packaging, transportation, treatment, disposal, remediation, etc.).

Enhancing technical capabilities

Sixteen technical workshops and study visits are planned to discuss/demonstrate methodologies and best practices covering different aspects of chemical, biological or radioactive waste management to increase capabilities and regional cooperation.

Stimulate cross-sectoral and international cooperation

As for all EU CBRN CoE Projects, one of the P67 objectives is to stimulate cooperation between the national and regional partners on CBRN issues. In order to achieve this, the engagement of multiple stakeholders is stimulated during the various activities implemented under P67, including regional workshops.

> **It is essential to provide entities working with hazardous materials resources to understand their legal and technical obligation**

■ IAEA Supporting Nuclear Safety Honduras

P67 is funded within the framework of the EU CBRN CoE initiative. The EU CBRN CoE Initiative involves 62 partner countries in eight regions. The European Commission (EC) leads the project, that is implemented with support from the EC's Joint Research Centre (JRC) and the United Nations Interregional Crime and Justice Research Institute (UNICRI). The project is implemented in close cooperation between experts from the ten partner countries of the South-East and Eastern European region, and by an EU consortium headed by the Sustainable Criminal Justice Solutions Europe (SCJS Europe). Other partners involved are, the Cranfield University, the International Security and Emergency Management Institute (ISEMI), the Nuclear and Decommissioning Company (JAVYS), Public Health England (PHE), and the Verification, Research, Training and Information Centre (VERTIC).

THE AUTHOR

Dr Hendrik Visser, PhD (Biophysical) Chemistry and MSc (Physical-Chemical, Chemical) Molecular Sciences, has over 20 years of experience in managing cooperative, international projects that deal with CBRN issues. He is Project 67 team leader. Besides that, he is the lead implementer of the EU CBRN CoE Project 53 (Strengthening the National Legal framework and Provision of Specialized Training on Bio-Safety and Bio-Security in Central Asian Countries). Since 2005, he has managed over 40 projects in Eastern Europe and Central Asia.

Between 2002 and 2005 he was a visiting scientist in the Russian Federation as part of an US Governmental sponsored visiting scientist program, to study the three-dimensional structure of membrane molecules of Yersinia Pestis using NMR spectroscopy. Before that he undertook a short post-doc at the Lawrence Berkeley National Laboratory after he had completed his PhD in Biophysical Chemistry at the University of California, Berkeley in 2001. He obtained his MSc degree in Molecular Sciences at the Wageningen Agricultural University (The Netherlands).

To contact him: hendrik.visser@scjs.eu
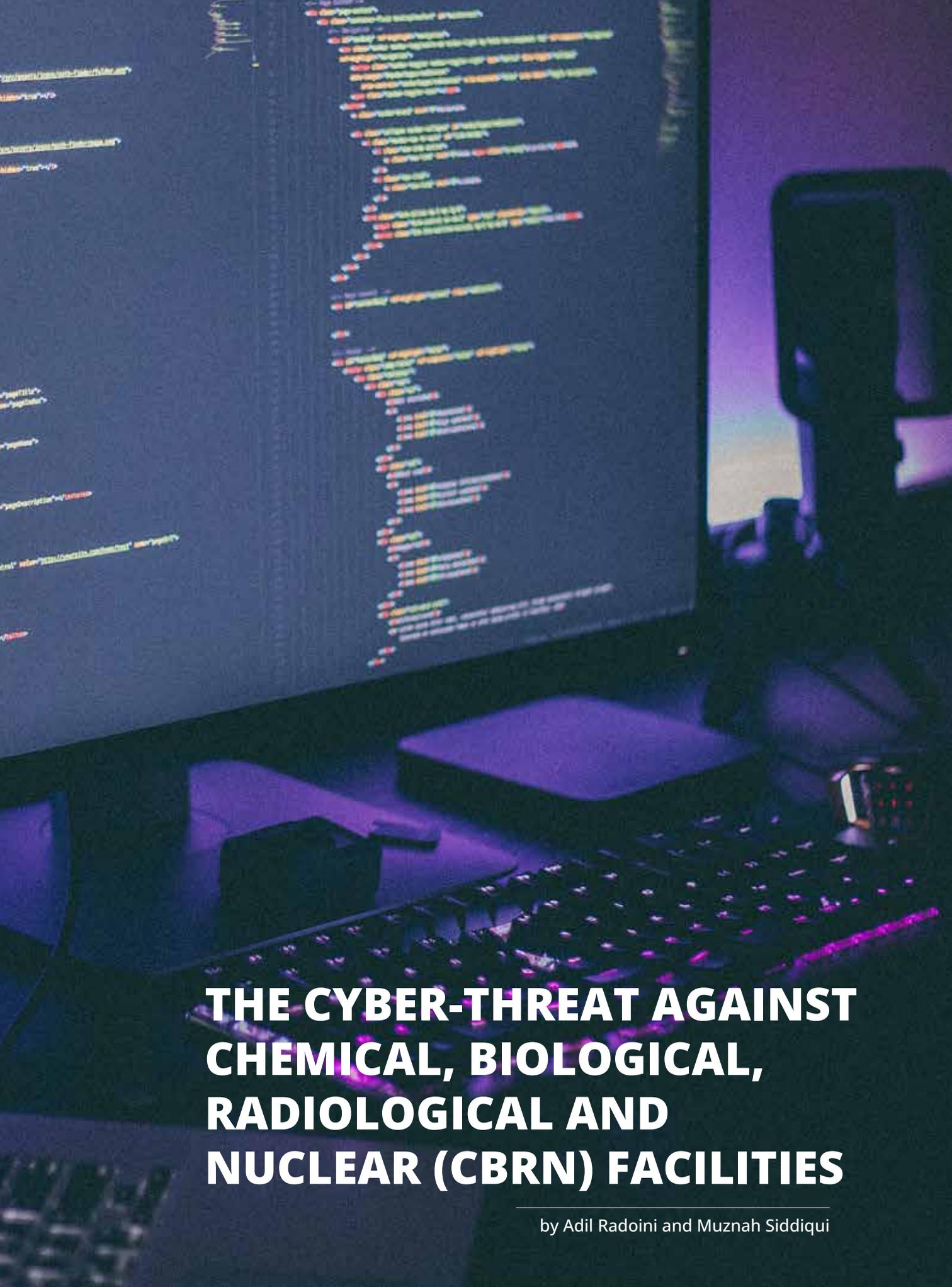
THE CYBER-THREAT AGAINST CHEMICAL, BIOLOGICAL, RADIOLOGICAL AND NUCLEAR (CBRN) FACILITIES

by Adil Radoini and Muznah Siddiqui

The increasing digitalization of critical infrastructure sectors and the associated industrial systems, particularly the digitalization of chemical, biological, radiological and nuclear (CBRN) facilities, is changing the nature of cyber-risks. In today's societies, entire ecosystems of key sector have become increasingly digital, decentralized and complex, multiplying opportunities and increasing the level and typology of threats.
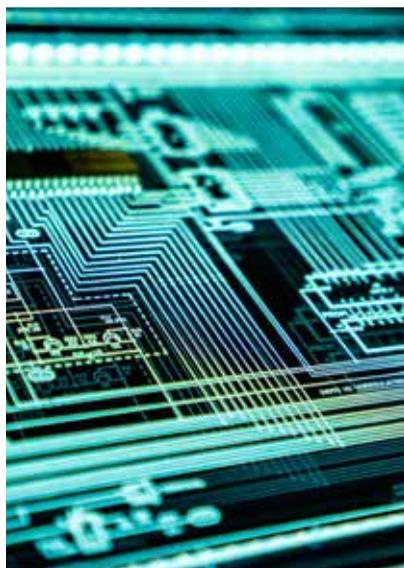
A recent major cyber-attack that should serve as a warning to us all about the scope these threats can have is the so-called *"SolarWinds cyber-attack" t*hat went undetected for months before Reuters[1] reported on it in December 2020. By first hacking into the U.S. company SolarWind, the massive hack successfully spread and infiltrated their customers' IT systems. Among them were U.S. Government agencies. SolarWinds is a Texas-based company whose software manages American companies, institutions, and government departments' administrative and security networks. The attack targeted parts of the Pentagon, the Department of Homeland Security, the State Department,

the Department of Energy, the National Nuclear Security Administration, and the Treasury. Other high-profile clients attacked included Fortune 500 companies such as Microsoft, Cisco, Intel, Deloitte, and organizations like the California Department of State Hospitals and the Kent State University.[2] According to high U.S .government officials, the scope of the damage is unprecedented and it could take years before the networks are secure again.[3]

A few weeks later, on 5 February 2021, a U.S. water treatment plant was targeted by a cyber-attack. An operator in Florida's West Coast saw his cursor being moved around on his computer screen, opening various software functions

that control the water treatment. The hackers increased by 100 times higher than normal the level of a chemical substance called sodium hydroxide - or lye - in the water supply.

Sodium hydroxide, the main ingredient in liquid drain cleaners, controls water acidity and removes metals from drinking water in treatment plants. Lye poisoning can cause burns, vomiting, severe pain and bleeding.[4]

> **"**
>
> **In today's societies, entire ecosystems of key sector have become increasingly digital, decentralized and complex, multiplying opportunities and increasing the level and typology of threats**

1   https://www.reuters.com/article/us-usa-cyber-treasury-exclsuive/suspected-russian-hackers-spied-on-u-s-treasury-emails-sources-idUKKBN28N0P-G?edition-redirect=uk

2   https://www.wsj.com/articles/solarwinds-hack-victims-from-tech-companies-to-a-hospital-and-university-11608548402?mod=djemalertNEWS

3   https://www.nytimes.com/2020/12/16/opinion/fireeye-solarwinds-russia-hack.html?action=click&module=Opinion&pgtype=Homepage

4   https://www.pewtrusts.org/en/research-and-analysis/blogs/stateline/2021/03/10/florida-hack-exposes-danger-to-water-systems

States, which is one of the most advanced countries in terms of cyber-security policies and preparedness in this area. All of this calls attention to the vulnerability of critical infrastructures to cyber-attacks across the world, as it poses a serious threat to the very functioning of entire sectors of our societies. Indeed, IBM, in a 2020 report, noted a 2000% increase in cyber-security incidents targeting the operational technologies employed in Critical National Infrastructures (CNI) since 2019.[6] The complexity of the interconnection of information systems in CNI is compounded by the COVID-19 pandemic, as it forced an abrupt shift for facilities and companies towards working from home. Consequently, the cyber-threat level has dramatically increased as production control networks have, for the most part, become remotely accessible.

Among all the critical infrastructures, special attention should be dedicated to the chemical, biological, radiological and nuclear facilities, considering the lethality, the pollution potential and the psychological impact that an attack involving CBRN material can provoke. Cyber threats can be engineered by various actors with differing intentions, including for instance

> **Cyber-sabotage could affect the normal operations of a CBRN facility or significantly damage equipment and processes**

More recently, in May 2021, another major cyber-attack targeted the U.S. Oil and Gas pipeline, disrupting the supply of almost half of the East Coast's fuel. According to the World Economic Forum, the attack caused an increase of oil prices and it is considered as one of the most expensive attacks to an economy.[5]

The recent attacks targeted objectives in the United

5   https://www.weforum.org/agenda/2021/05/cyber-attack-on-the-us-major-oil-and-gas-pipeline-what-it-means-for-cybersecurity/

6   https://securityintelligence.com/posts/what-the-explosive-growth-in-ics-infrastructure-targeting-means-for-security-leaders/

the physical sabotage and destruction of infrastructures and processes by creating deliberate malfunctions. In the case of CBRN facilities, the consequences could be life-threatening. Furthermore, computer hackers may seek to disclose critical information, render information systems unavailable to authorized users or prevent the proper update of information. The objectives of the criminal actors involved in these operations may include the wish to build access points in facilities for further uses, spreading fear among the public and undermining the credibility of governments.

A cyber-attack against a CBRN facility can disable the IT system and allow the theft of sensitive data. But the breach can also serve as a stepping stone to prepare other types of attacks involving CBRN materials. In addition, cyber-sabotage could affect the normal operations of a CBRN facility or significantly damage equipment and processes. The attacks themselves can occur by injecting malware or viruses into systems, thereby posing a considerable threat to the supply chain management cycles. Finally, cyber espionage refers to retrieving confidential information for malicious purposes. This form

of threat is more common, as it requires a lower level of technical expertise, several tools are also freely available on the Internet, such as spyware systems.

The types of malicious actors range from terrorists, covert agents and disgruntled employees to state/non-state hackers, militant opponents, or recreational hackers. In the case of the former, several terrorist groups have begun using social media to recruit hackers and radicalize CBRN facility employees who could enormously facilitate the effort of obtaining sensitive information on the IT system of the facilities. For instance, ISIL successfully radicalized an employee of the Doel nuclear power plant in Belgium, who eventually left the country to partake in terrorist activities.[7] Moreover, the FBI highlights the additional concern that terrorists may hire hackers to conduct cyber-attacks in conjunction with conventional attacks.

A cyber-attack against a nuclear facility could potentially corrupt nuclear command and control systems whilst potentially allowing for the release or theft of radioactive material. The Nuclear Threat Initiative documented 16 cas-

es of cyber-attacks against nuclear facilities across the world. Among the targeted countries there were Lithuania, the UK, the U.S, Japan, Syria, Iran, South Korea and Germany (see table below).

The urgency for a cyber-chemical security framework is compounded by the fact that virtually all chemical plants have some type of computer-based automated control systems and also because the communication networks are replaced or complemented with wireless networks, and to point-to-point communications. In most cases, the chemical industry self-regulates, and whilst they invest in their cyber-security, national governments ought to step in and create standardized norms and regulations.[8]

A recent study that researched the opinion of international field leaders in biotechnology and cybersecurity concluded that "the issue of cyber-bio-security is not well-known or understood, even among biotechnology and cybersecurity experts." Accordingly, the issue of cyber security in the field of biology have not been effectively fleshed out in a practical manner, thereby creating vulnerabilities at the apex of

7   https://www.washingtonpost.com/world/europe/brussels-attacks-stoke-fears-about-security-of-belgian-nuclear-facilities/2016/03/25/7e370148-f295-11e5-a61f-e9c95c06edca_story.html

8   https://www.aiche.org/academy/videos/conference-presentations/detection-cyber-attacks-and-resilient-operation-nonlinear-processes-under-economic-model-predictive

life and medical sciences and infrastructure systems.[9] The increased reliance on Internet connections of facilities containing sensitive bio-data that could be used maliciously to create or modify bio-agents and pathogens should be considered as a severe threat globally.

UNICRI is currently identifying assessment methodologies, tools and good practices that can be made available to the United Nations Member States to improve the governance of cyber-threats against CBRN facilities. The various types of threats and malicious actors involved highlight the need to develop a set of standardized good practices to prevent attacks against CBRN facilities. These practices can be divulged through general awareness-raising and training activities addressed to decision-makers, managers and operators. Such activities can provide the relevant stakeholders with the tools needed to identify potential emerging threats. Facilities can use various methods, including simulations and tests, to enhance knowledge among staff. This will prepare them to identify

potential vulnerabilities; evaluate the impact of attacks; recognize the need for constant vigilance; establish protection mechanisms during attacks; develop cyber-resilience and ascertaining the importance of cyber-security instruments. Through embedding awareness of the risks of cyber-threats across operational, managerial and decision-making levels, the most exploited vulnerabilities of CBRN facilities can be consequently considerably reduced.

Furthermore, robust and effective legislation is a prerequisite for developing effective cyber-security frameworks to secure CBRN critical infrastructures. Accordingly, relevant legislative bodies may authorize national cyber-security programs which address the CBRN risk whilst incorporating adequate deterrent and enforcement measures. In addition, an appropriate legislation should address emerging forms of cyber-threats and vulnerabilities whilst potentially establishing voluntary standards in partnership with the private sector. Consequently, an

important element of a risk mitigation strategy should envisage the involvement of experts in cyber-physical security, science, intelligence, law enforcement, state communication departments etc., in a collaborative process. This holistic and multi-stakeholder approach will ensure the full breadth of issues are covered. Finally, relevant legislation and regulations could establish clear consequences for non-compliance, particularly given the magnitude of the potential risks. Other forms of governance measures could include education and training for personnel, the establishment of ad-hoc policies, structures and processes (such as regular assessments and inter-agency coordination), alongside the allocation of resources towards investing in cyber-security infrastructures, in particular for CBRN facilities.

UN Member States have engaged in important efforts to protect their societies from CBRN threats. It is now time for them to get prepared and prevent CBRN risks coming from the cyber-dimension.

---

9   https://www.sciencedirect.com/science/article/pii/S2590053620301129#bb0040

❯ Chronology of cyber-attacks to nuclear facilities[10]

#	MONTH/YEAR	NAME	COUNTRY	DESCRIPTION	CATEGORY
1	February 1992	Ignalina Nuclear Power Plant	Lithuania	Employee attempted sabotage	Intentional
2	June 1999	Bradwell Nuclear Power Plant	United Kingdom	Employee altered/destroyed data	Intentional
3	March, 2002	Davis-Besse Nuclear Power Station	United States	Worm	Intentional
4	June 2005	Japanese Nuclear Power Plants	Japan	Data release	Unknown
5	December 2006	Syrian Nuclear Program	Syria	Espionage	Intentional
6	March 2009	Energy Future Holdings	United States	Employee attempted sabotage	Intentional
7	June 2010	Natanz Nuclear Facility	Iran	Stuxnet virus used to destroy centrifuges	Intentional
8	April 2011	Oak Ridge National Laboratory	United States	Data theft via spear-phishing	Intentional
9	October 2011*	Natanz Nuclear Facility	Iran	Duqu virus used to conduct espionage	Intentional
10	May 2012	Natanz Nuclear Facility	Iran	Flame virus used to conduct espionage	Intentional
11	January 2014	Monju Nuclear Power Plant	Japan	Data release	Unknown
12	December 2014	Korea Hydro and Nuclear Power Company	South Korea	Data theft and release	Intentional
13	February 2015	Japanese nuclear material control center	Japan	Nuclear facility used as relay point in cyberattack	Unknown
14	February 2016*	Nuclear Regulatory Commission/U.S. Department of Energy	United States	An employee attempted to infect government computers with viruses distributed via spear-phishing emails	Intentional
15	April 2016	Gundremmingen Nuclear Power Plant	Germany	Two viruses entered the plant's fuel rod monitoring system	Unknown
16	June 2016	University of Toyama, Hydrogen Isotope Research Center	Japan	Data theft via spear-phishing	Intentional

THE AUTHORS

Adil Radoini is the United Nations Interregional Crime and Justice Research Institute (UNICRI) Regional Coordinator for the Middle East and Gulf Cooperation Countries. He works for the Chemical, Biological, Radiological and Nuclear (CBRN) and Security Governance Programme. He previously worked as a journalist for the Italian press and television sectors. In 2009, together with other international experts, he published "Un Hussein alla casa Bianca", a perspective of the Arab world on the 2008 U.S. elections. He graduated from the University of Bologna with a Master's degree in International Relations focusing on Middle Eastern politics, carrying out a research thesis led in Cairo and at the Institut d'Etudes Politiques in Paris.

Muznah Siddiqui is a graduate from the University of Cambridge, and has completed her Master's in International Relations and Politics. She is currently working as an intern at the United Nations Office of Counter-Terrorism, and her research interests include the protection of human rights, cyber-security and countering violent extremism.

> **A study of healthcare cyberattacks in over 30 countries shows the scale of the rising threat**

▸ **A study of healthcare cyberattacks in over 30 countries shows the scale of the rising threat.**

▸ **Ransomware attacks dominate the broadening scope of threats to healthcare providers.**

▸ **More action is needed from actors in the sector, cybersecurity firms and governments to ensure access to healthcare.**

INFOCUS

by Stéphane Duguin

IF HEALTHCARE DOESN'T STRENGTHEN ITS CYBERSECURITY, IT COULD SOON BE IN CRITICAL CONDITION

It's hard to imagine anything more cynical than holding a hospital to ransom, but that is exactly what's happening with growing frequency. The healthcare sector is a popular target for cyber-criminals. Unscrupulous attackers want data they can sell or use for blackmail, but their actions are putting lives at risk. A cyberattack on healthcare is more than an attack on computers. It is an attack on vulnerable people and the people who are involved in their care; this is well illustrated by the breadth of healthcare or-ganizations, from hospitals to mental health facilities to pharmaceutical companies and diagnostic centres, targeted between June 2020 and September 2021.

Cyberattacks on healthcare have continued to plague the sector since the start of the COVID-19 pandemic. At the CyberPeace Institute, we have analyzed data on over 235 cyberattacks (excluding data breaches) against the healthcare sector across 33 countries. While this is a mere fraction of the full scale of such at-

"

Healthcare cybersecurity suffers from a general lack of human resources

tacks, it provides an important indicator of the rising negative trend and its implications for access to critical care.

Over 10 million records have been stolen, of every type, including social security numbers, patient medical records, financial data, HIV test results and private details of medical donors. On average, 155,000 records are breached during an attack on the sector, and the number can be far higher, with some incidents reporting the breach of over 3 million records.

Poor bill of health

Ransomware attacks on the sector, where threat actors lock IT systems and demand payment to unlock them, have a direct impact on people. Patient care services are particularly vulnerable; their high dependence on technology combined with the critical nature of their daily operations means that ransomware attacks endanger lives. Imagine being in an ambulance that is diverted because a cyberattack has caused chaos at your local emergency department. This is not a hypothetical situation. We found that 15% of ransomware attacks led to patients being redirected to other facilities, 20% caused appointment cancellations, and some services were disrupted for nearly four months.

Ransomware attacks on the sector occurred at a rate of four incidents per week in the first half of 2021, and we know

this is just the tip of the iceberg, as there is a significant absence of public reporting and available data in many regions. Threat actors are becoming more ruthless, often copying the data, and threatening to release it online unless they receive further payment.

Health records are low-risk, high reward targets for cybercriminals – each record can fetch a high value on the underground market, and there is little chance of those responsible being caught. Criminal groups operate across a wide range of jurisdictions and regularly update their methods, yet we continue to see that attackers act with impunity.

Securing the right to healthcare

We can, and should, be doing better. The first step is with cybersecurity itself. Healthcare cybersecurity suffers

Incidents over time by healthcare sub-sectorImage: CyberPeace Institute

from a general lack of human resources. More people need to be trained and deployed.

Software and security tools need to be secure by design. This means putting security considerations at the centre of the product, from the very beginning. Too often security options are added as a final step, which means they paper over inherent weaknesses and loopholes.

Healthcare organizations should also do more, particularly increasing their investment in cybersecurity to secure infrastructure, patch vulnerabilities and update systems, as well as building and maintaining the required level of cybersecurity awareness-raising and training of staff. Healthcare organizations also need to commit to due diligence and standard rules of incident handling.

But these matters are ultimately too big for individual organizations to solve alone. Governments must take proactive steps to protect the healthcare sector. They must raise the capacity of their national law enforcement agencies and judiciary to act in the event of extraterritorial cases so that threat actors are held to account. This requires the political will and international

Governments must take proactive steps to protect the healthcare sector

cooperation of governments, including for investigation and prosecution of threat actors.

One point of real concern from our analysis is that information about cyberattacks, such as ransomware incidents, is inadequate due to under-reporting and lack of documentation of attacks. Thus it is impossible to have a global view of the extent of cyberattacks against the healthcare sector. To build even a partial picture of such attacks meant us accessing and aggregating the data that ransomware operators – the criminals – publish or leak online.

It is not acceptable that they are the significant source of information relating to cyber incidents and threats posed to the sector. We want to shift away from data published by or from malicious actors and

encourage stronger reporting and transparency relating to cyberattacks by the healthcare sector to improve both the understanding of the threat and the ability to take appropriate action to reduce it.

Our analysis shows that 69% of countries for which we have recorded attacks have classified health as critical infrastructure. Healthcare must be recognized as critical infrastructure globally. Designation as critical infrastructure would ensure that the sector is part of national policies and plans to strengthen and maintain its functioning as critical to public health and safety.

Governments must enforce existing laws and norms of behaviour to crack down on threat actors. They should cooperate with each other to

ensure that these laws are put into operation in order to tackle criminals that operate without borders. More should be done to technically attribute cyberattacks to identify which actors have carried out and/or enabled the attack.

Health is a fundamental human right. It is the responsibility of governments to lead the way in protecting healthcare. People need access to reliable, safe healthcare, and they should be able to access it without worrying about their privacy, safety and security.

We hope there is global recognition that the status quo is unacceptable and that we can all do more to prevent cyberattacks against healthcare, protect the victims of such attacks, and hold perpetrators to account.

"

Information about cyberattacks, such as ransomware incidents, is inadequate due to under-reporting and lack of documentation of attacks

THE AUTHOR

Stéphane Duguin is the Chief Executive Officer of the CyberPeace Institute. He has spent two decades analysing how technology is weaponized against vulnerable communities. In particular, he has investigated multiple instances of the use of disruptive technologies, such as AI, in the context of counter terrorism, cybercrime, cyberoperations, hybrid threats, and the online use of disinformation techniques. He leads the CyberPeace Institute with the aim of holding malicious actors to account for the harms they cause. His mission is to coordinate a collective response to decrease the frequency, impact, and scale of cyberattacks by sophisticated actors.

Prior to this position, Stéphane Duguin was a senior manager and innovation coordinator at Europol. He led key operational projects to counter both cybercrime and online terrorism, such as the European Cybercrime Centre (EC3), the Europol Innovation Lab, and the European Internet Referral Unit (EU IRU). He is a thought leader in digital transformation and convergence of disruptive technologies. With his work published in major media, his expertise is regularly sought in high-level panels where he focuses on the implementation of innovative responses to counter new criminal models and large-scale abuse of cyberspace.

This contribution, authored by Stéphane Duguin, Chief Executive Officer at CyberPeace Institute, *was originally published by the World Economic Forum. The CyberPeace Institute is an independent non-governmental organization headquartered in Geneva.*

Five years of global academic collaboration building evidence for sexual and reproductive health and rights policies

ANSER

A Ghent University led initiative
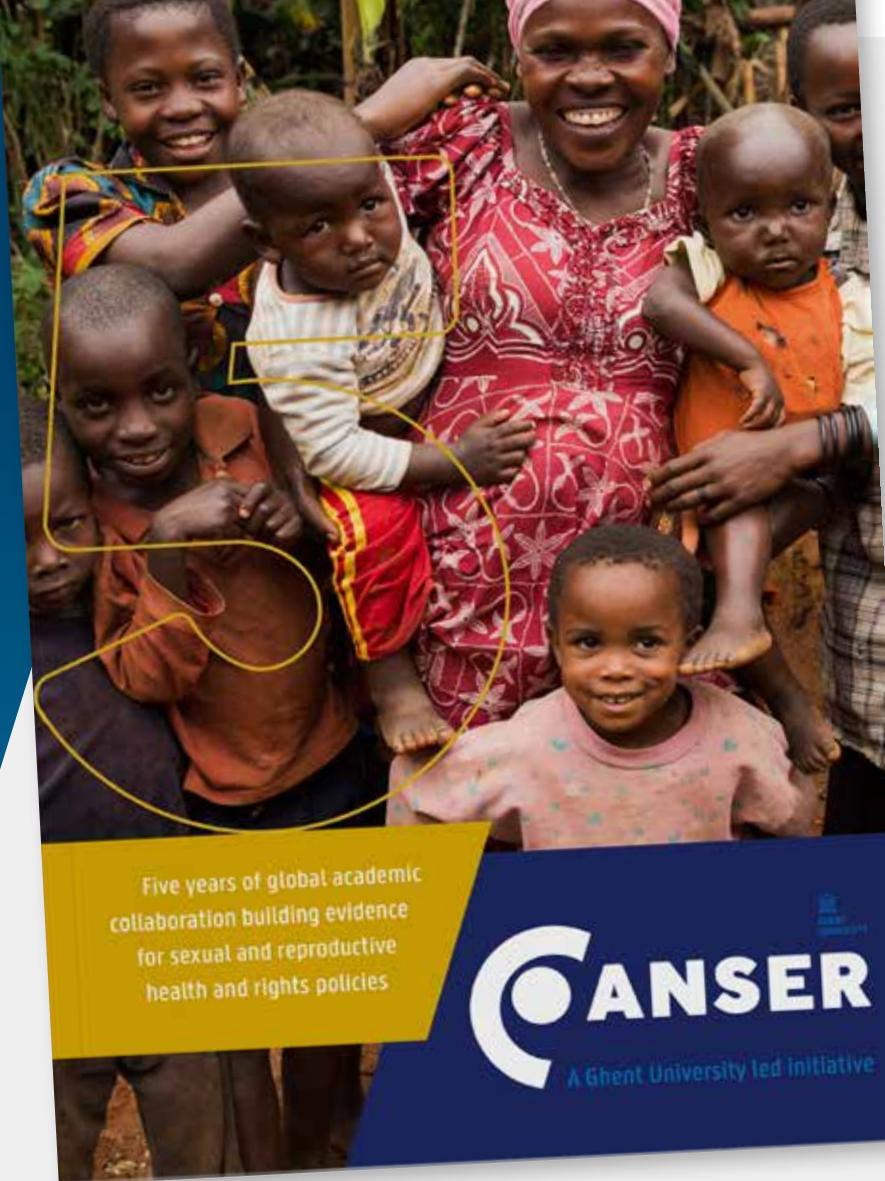
Hardyns, W., Thys, J., Dorme, L., Klima, N., & Pauwels, L. (2021). Multi-agency working to prevent violent radicalisation. *RADICES, 1*(1), 22–40.

Dewinter, M., Vandeviver, C., Dau, P. M., Vander Beken, T., & Witlox, F. (2021). The impact of strict measures as a result of the COVID-19 pandemic on the spatial pattern of the demand for police: case study Antwerp (Belgium). *Crime Science, 10*(1).

Aga, N., Rowaert, S., Vander Laenen, F., Vandevelde, S., Vander Beken, T., Audenaert, K., & Vanderplasschen, W. (2021). Connectedness in recovery narratives of persons labeled not criminally responsible: a qualitative study. *International Journal of Forensic Mental Health, 20*(3), 303–316.

Rummens, A., Snaphaan, T., Van de Weghe, N., Van den Poel, D., Pauwels, L., & Hardyns, W. (2021). Do mobile phone data provide a better denominator in crime rates and improve spatiotemporal predictions of crime? *ISPRS International Journal of Geo-Information, 10*(6), 369.

De Pelecijn, L., Decoene, S., & Hardyns, W. (2021). 'If I said I trust you, I would be lying': reflections and recommendations for conducting interviews with (violent) extremist prisoners. *Journal for Deradicalization*, (27), 284–310.

Sas, M., Hardyns, W., van Nunen, K., Reniers, G., & Ponnet, K. (2021). Measuring the security culture in organizations: a systematic overview of existing tools. *Security Journal*.

Colman, C., Blomme, E., Ducheyne, A., Vander Laenen, F., & Wittouck, C. (2021). L'importance du screening pour un fonctionnement efficace de la chambre de traitement de la toxicomanie. In B. Mine (Ed.), *La récidive*

Open Access

RESEARCH

The impact of strict measures as a result of the COVID-19 pandemic on the spatial pattern of the demand for police: case study Antwerp (Belgium)

Abstract

Keywords: Spatial point pattern test, Police demand, Lockdown, Street segments, Emergency call data

BMC

---
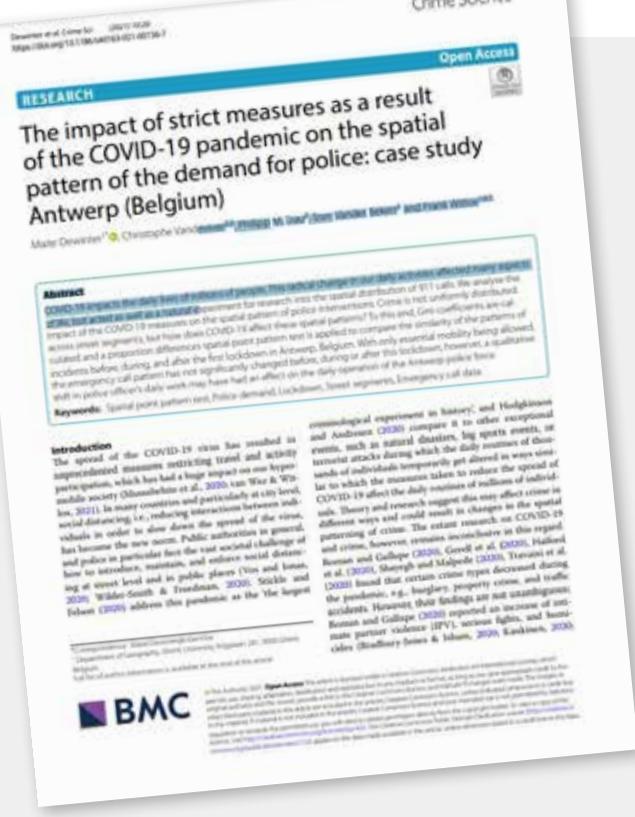
et les carrières criminelles en Belgique. Politeia.

Chatzinikolaou, A., & Lievens, E. (2021). Sexting amongst children and teenagers: towards a policy that balances protection and autonomy. *ANSER: five years of global academic collaboration building evidence for sexual and reproductive health and rights policies*. ANSER.

Milkaite, I., De Wolf, R., Lievens, E., De Leyn, T., & Martens, M. (2021). Children's reflections on privacy and the protection of their personal data: a child-centric approach to data protection information formats. *Children and Youth Services Review, 129*.

Lembrechts, S., & Desmet, E. (2021). Communication 56/2018: V.A. v. Switzerland: rights of accompanied children in asylum proceedings: the challenges of a holistic approach and high quality decision-making. *Leiden Children's Rights Observatory*. Leiden.

Beeson, M., & Biscop, S. (2021). EU–Asia security relations in a global context: geoeconomics and geopolitics. In T. Christiansen, E. Kirchner, & S. S. Tan (Eds.), The European Union's security relations with Asian partners (pp. 29–49). Palgrave Macmillan.

Biscop, S. (2021). Analysing the EU global strategy on foreign and security policy. In J. Rehrl (Ed.), Handbook on CSDP: the common security and defence policy of the European Union (Fourth edition, pp. 29–36). Vienna: Ministry of Defence of the Republic of Austria.

Micheletto, L. (2021). *Hate crime legislation and the limits of criminal law: a principled and evidence-based assessment of hate crime law and its application to Italy*. Universiteit Gent. Faculteit Recht en Criminologie.

Van Impe, M. (2021). *Stigma through the eyes of people who use(d) illegal drugs: challenging boundaries through Participatory Action Research*. Ghent University. Faculty of Law and Criminology.

Leloup, P., & Cools, M. (2021). (Post-)crisis policing, public health and private security: the COVID-19 pandemic and the private security sector. *Policing and Society*, 1–16.

Spiritus-Beerden, E., Verelst, A., Devlieger, I., Langer Primdahl, N., Botelho Guedes, F., Chiarenza, A., De Maesschalck, S., Durbeej, N., Garrido, R., Gaspar De Matos, M., Ioannidi, E., Murphy, R., Oulahal, R., Osman, F., Padilla, B., Paloma, V., Shehadeh, A., Sturm, G., Van den Muijsenbergh, M., Derluyn, I. (2021). Mental Health of Refugees and Migrants during the COVID-19 Pandemic: The Role of Experienced Discrimination and Daily Stressors. *International Journal of Environmental Research and Public Health, 18*(12), 6354.

De Haan, M., & Destrooper, T. (2021). Using restorative justice to rethink the temporality of transition in Chile. *The International Journal of Restorative Justice, 4*(2), 206–228.

De Coninck, J. (2021). *Catch-22 in the law of responsibility of international organizations: systemic deficiencies in the EU responsibility paradigm for unlawful human rights conduct in integrated border management*. Ghent University. Faculty of Law and Criminology.

THE DUMB AND THE DANGEROUS ROAD AHEAD

by Hedi Nasheri[1]

The current state of world affairs is extremely alarming. The geopolitical tensions, global power struggles, conflicts in cyberspace, the global impact of the Covid-19 pandemic, cyber-attacks, the rise of far-right nationalist and extremist groups, the climate challenges, food and water security and the migration crisis are among many pressing factors impacting the world order, democracies and the global security.

As emerging technologies such as artificial intelligence, biotechnology, and quantum technology, as well as new weapons technologies such hypersonic weapons and directed energy weapons, continue to mature, they could hold significant implications for societies around the world.

While emerging technologies such as artificial intelligence (AI), often combined with related technologies such as robotics, have led to positive impact, among the others, in the field of medicine, transportation, telecommunications, housing, and have significantly contributed to scientific discoveries, at the same time these technologies, if not properly governed and used, could pose a threat to civilization and humanity as we know it. Highlighting the real risks associated with the misuse of AI can help understanding the current status of this technology and its potential negative consequences. At the time of writing this piece, the following major events occurred which highlights the good, the bad and the ugly side of emerging technologies such as AI. These technologies, which characterize the Fourth

1   Hedi Nasheri, is a Professor of Criminology and Justice Studies at Kent State University in the United States.

Industrial Revolution and are driving profound changes in society and the economy need safeguard mechanisms.

The first 3D housing community was completed and operational in Mexico. This is a housing development that can withstand climate challenges such as earthquakes and harsh weather. At the same time, we learned that Facebook is unintentionally spreading misinformation through the company's algorithms. Given the current geopolitical environment it is not surprising that AI poses profound changes to society. This emerging technology requires constant safeguard at every level and ongoing accountability to prevent its misuse. Although there is an enormous and growing number of policy initiatives to try to keep the potential for harm in check, such measures may be insufficient. Some researchers point out that the tech sector have been naïve about the technology they champion, how it will actually be used and what consequences their technological innovations will have.

Some of the problems this article highlights exist with or without AI, but new technological advances such as AI have the potential to magnify them at a level we cannot predict. This is why is so crucial to develop normative frameworks in order to make sure

that developments in this field respond to the principles of lawfulness, social acceptance, trustworthiness, responsibility and ethics.

The race to develop, commercialize and distribute

Ambitious corporations in the industrialized advanced nations driven by profit and greed are commercializing, developing and deploying AI on large scale. The distribution and production of robots for a wide range of use, such as autonomous weapon systems, pizza delivery drones, driverless delivery trucks, sex robots, recreational pets, cleaning robots, security application, competitive racing, photography, facial recognition software and surveillance technology are advertised and sold. AI has received considerable attention globally as a tool that can process vast quantities of data, discover patterns and correlations in the data unseen to the human eye. It is capable of enhancing effectiveness and efficiency in the analysis of complex information.

Humanitarian, recreational, military, and commercial applications of robots are truly global in nature. In light of this accelerated distribution and production, there is a growing interest amongst law enforcement and counter-terrorism agencies around the world in exploring AI technology. It is likely that the growth of these technologies will produce a new world.

Our changing world

In 2018 the London Times printed an editorial from Stephen Hawking, warning us that AI will likely outsmart humans. According to Hawking's legacy, AI will either be the best thing that is ever happened to us, or it will be the worst thing. If we are not careful, it very well may be the latter. Another important figure in the business circles, Elon Musk believes that AI is

Ambitious corporations in the industrialized advanced nations driven by profit and greed are commercializing, developing and deploying AI on large scale
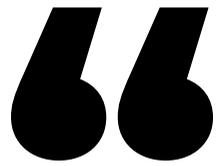
According to Hawking's legacy, AI will either be the best thing that is ever happened to us, or it will be the worst thing

more dangerous than nuclear warheads and must be regulated. Musk believes that the race for AI could be the cause for World War III. He bases his belief on the past century of human behavior in regard to warfare. With developments such as Google's AlphaGo, Musk has seen how fast AI can improve without anyone predicting the rate of speed as well as its capabilities.[2]

The development of AI is largely unchecked and many feel insufficient attention is given to its potential to create problems.[3] AI researchers warn that AI can develop negative behaviors based on their interactions with humans, they give examples of human induced negative behaviors. AI, as creations of humans can intrinsically absorb problems that their creators have not solved yet. This involves the replication of human problems in the solutions created by AI.

2   Barbaschow, A. (2018). AI 'more dangerous than nukes': Elon Musk still firm on regulatory oversight. Retrieved 2020, from https://www.zdnet.com/article/more-dangerous-than-nukes-elon-musk-still-firm-on-regulatory-oversight-of-ai/?ftag=TRE6a12a91&bhid=28036118512285295119801408296132

3   Leprince-Ringuet, D. (2021). US, China or Europe? Here's Who is Really Winning the Global Race for AI.

Without the right governance measures in place there is a risk that AI can result in anti-social or harmful actions.[4] At the same time, AI is being deployed as a weapon in modern militaries. AI is being integrated into weapons and used in automated vehicles, like unmanned aerial vehicles (UAVs), or small land vehicles. The dynamics between AI and social media also raise questions in terms of possible misuse to manipulate social media users.

There are only a handful of countries that have made striking advancement in the designing and production of AI technologies and the current debate is on who is leading the way. Recent reports suggest that some countries are exponentially progressing while others are still in an embryonic phase. This will contribute to widen the existing gap among countries in terms of development and progress.

There are also different approaches to AI: some countries have surpassed others in the area of defense - posing a major concern for the future of warfare – some others want to acquire the leadership in the development of AI, believing that AI is the focus of international competition and economic development. A prominent politician stated that whoever leads AI will rule the world.

A typical case of concern is the following: a country collects data from electric cars by claiming that the data is used for policy planning but there are obvious privacy implications. Auto makers worry the data could be used for industrial espionage but yet they comply with the laws so they can sell their cars in the country.[5] Using surveillance to suppress dissent and facial recognition technology for mass surveillance purposes is also a case of concern.[6] Government officials use terrorist attacks as a justification for mass surveillance programs, despite the evidence that they do not meet the original expectations. Most of these programs are kept secret so little is known about the success rate. However, informa-

4   Waddell, K. (2018). AI might need a therapist, too. Retrieved 2020, from https://www.axios.com/ai-might-need-a-psychologist-1529700757-a21b0d80-727a-402f-91d8-3196150d59ed.html?utm_source=newsletter&utm_medium=email&utm_campaign=newsletter_axiospm&stream=top

5   Kinetz, E. (2018). In China, your car could be talking to the government. Retrieved 2020, from https://apnews.com/4a749a4211904784826b45e812cff4ca?utm_source=newsletter&utm_medium=email&utm_campaign=newsletter_axiosam&stream=top

6   LeVine, S. (2019). A paradise for the age of the techno-autocrat. Retrieved 2020, from https://www.axios.com/us-china-artificial-intelligence-surveillance-addd458b-2e0e-4309-91d8-187aabc83814.html?utm_source=newsletter&utm_medium=email&utm_campaign=newsletter_axiosam&stream=top

tion that has been disclosed does not justify mass surveillance.[7]

National security risks

As academic institutions, major corporations, and government science and technology programs continue to develop and deploy AI capabilities, AI-enhanced systems will be trusted with increasing levels of autonomy and decision making, presenting the world with a host of economic, military, ethical, and privacy challenges. Furthermore, interactions between multiple advanced AI systems could lead to unexpected outcomes that increase the risk of economic miscalculation or battlefield surprise.

Artificial intelligence, digital security, physical security, and political security are inherently intertwined and connected. As AI systems extend further into domains commonly believed to be uniquely human (like social interactions), more sophisticated social engineering attacks will happen based on these capabilities. AI, if not properly designed and used, will significantly change the political power balance. It is

> ## " AI, if not properly designed and used, will significantly change the political power balance

not clear what the long-term implications of malicious uses of AI will be. Production and detection of misleading information, interference with elections, an epidemic of computer viruses only scratch the surface of the types of political and stability security risks.

In his message8 the Secretary-General of the United Nations, António Guterres said: "machines with the power and discretion to take lives without human involvement are politically unacceptable, morally repugnant and should be prohibited by international law". Despite the many initiatives, including the United Nations Convention on Certain Conventional Weapons Group of Governmental Experts, so far, limited progress has been made in the adoption of new

legally binding rules to regulate lethal autonomous weapons (LAWs). It appears that too many nations are not likely to enter into a treaty that would ban the use of AI decision making in weapons.

In the past several years we have seen that AI has been used to attack elections in different parts of the world. AI could become a growing threat to national security. The use of AI driven cyberattacks that can evade detection and use of AI driven phishing attacks are some examples of the types of threats. More advanced nations' intelligence agencies are working with the private sector to aide them in the development of defense AI systems.[9] Researchers expect that AI will be used to create more sophisticated malware. They expect that AI will be used in phishing, vulnerability recognition and autonomous attacks.[10] There are other threats such as AI being able to reproduce the biases of humans. AI is capable of creating, attacking or being misused such as, deepfakes, disrupting other AI controlled systems, large scale blackmail, fake news, misuse of military robots, learning

7   Kirchner, L. (2015). What's the Evidence Mass Surveillance Works? Not Much. Retrieved 2020, from https://www.propublica.org/article/whats-the-evidence-mass-surveillance-works-not-much?utm_source=newsletter&utm_medium=email&utm_campaign=newsletter_axiosdeepdives&stream=top

8   https://news.un.org/en/story/2019/03/1035381

9   Macaulay, T. (2020). UK spies must ramp up use of AI to fight new threats, says report. Retrieved 2020, from https://thenextweb.com/neural/2020/04/27/uk-spies-must-ramp-up-use-of-ai-to-fight-new-threats-says-report/

10   Osborne, C. (2018). This is how artificial intelligence will become weaponized in future cyberattacks. Retrieved 2020, from https://www.zdnet.com/article/this-is-how-artificial-intelligence-will-become-weaponized-in-future-cyberattacks/?ftag=TRE-03-10aaa6b&b-hid=28036118512285295119801408296132
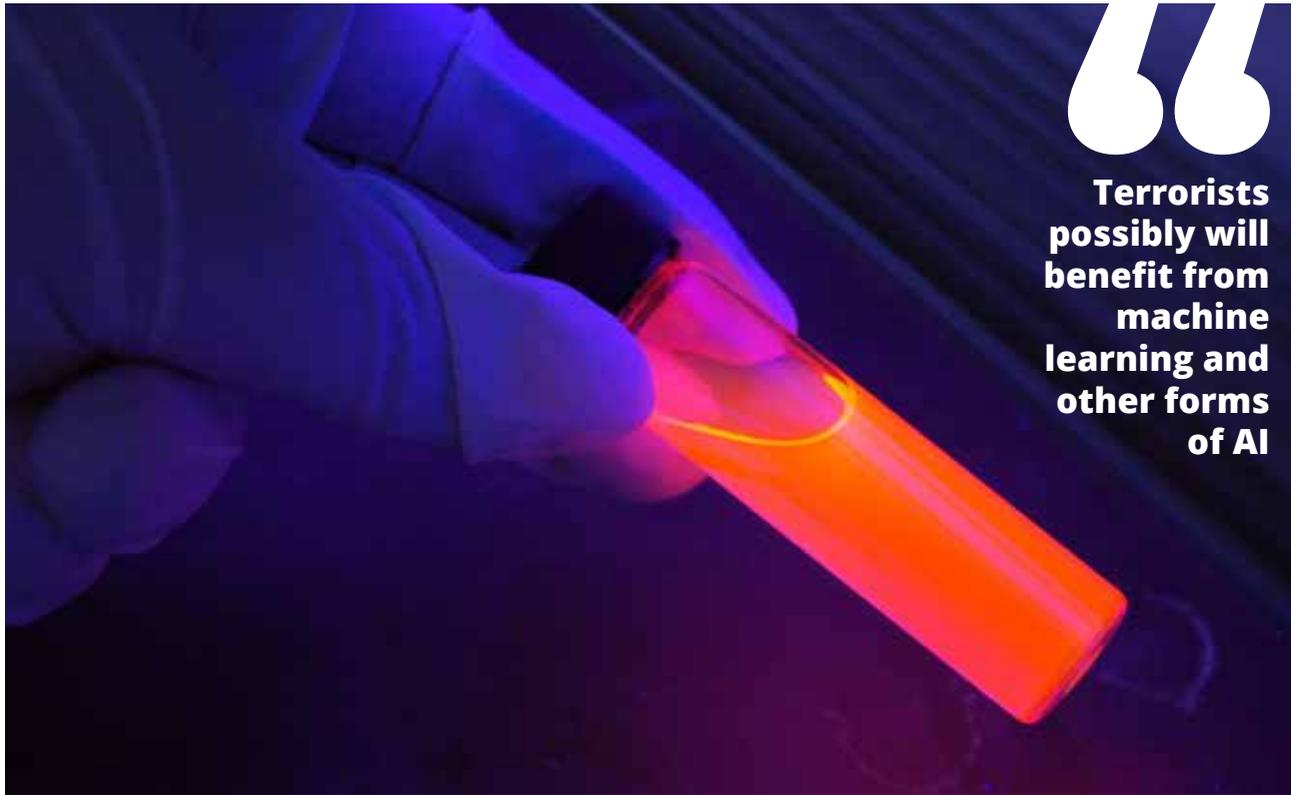
> **Terrorists possibly will benefit from machine learning and other forms of AI**

based cyber-attacks, autonomous drones attack, distributed denial-of-service (DDoS) attack, defeating facial recognition and the stock market manipulation.[11]

Terrorism and emerging technology

New technologies such as AI around the world can put sophisticated capabilities in the hands of individuals, state actors and nations. It is critical to understand the security implications for the advances in emerging technologies such as biotechnology and AI. A disturbing trend is the reported attempts of state- and non-state actors to acquire and use chemical and biological weapons in blatant violations of international norms.

It is likely that terrorist organizations will use AI. Terrorists possibly will benefit from machine learning and other forms of AI, for instance in the preparations for their military operations and for the gathering of information. Particularly when carrying out cyber-attacks, automated tasks executed by using AI can make the scale and impact of these attacks potentially larger. AI technologies are sold to and used by instable states, not to mention the role that organized crime groups can play in this scenario. It is unlikely that at this time terrorist organizations will have the capabilities to develop and maliciously use AI technology, however,

---

11   Leprince-Ringuet, D. (2020). AI vs your career? What artificial intelligence will really do to the future of work. Retrieved 2020, from https://www.zdnet.com/article/ai-vs-your-career-what-artificial-intelligence-will-really-do-to-the-future-of-work/?ftag=TRE6a12a91&bhid=2803611851228529511980140 8296132&mid=12774060

Salisbury, United Kingdom
A military-grade nerve agent - Novichok - was used in the attempt to assassinate Sergei Skripal. MAR. 2018

Tbilisi, Georgia
A toxic chemical was used at the Tbilisi International Airport.
JUL 2018

Syria
Chemical weapons – including chlorine and sarin – were repeatedly used despite acceding to the Chemical Weapons Convention in 2013.
2013-2018

Syria and Iraq
ISIS has used sulfur mustard and toxic industrial chemicals against its opponents in Syria and Iraq.
2014-2017

Kuala Lumpur, Malaysia
Kim Jong Un's half brother was assassinated by the nerve agent VX.
FEB 2017

Chemical Attacks Since 2013

they can possess this technology. An example: when an unstable state collapses due to internal conflicts, the chances that these technologies will end up in the hands of terrorist and criminal organizations is very likely.

Chemical and biological weapons

In the recent years, some countries, and terrorist groups such as ISIS have used chemical weapons on the battlefield or in sponsored assassination operations (the responsibility of state actors is under investigation). These attacks have included traditional chemical weapon agents, toxic industrial chemicals, and the first known use of a Novichok nerve agent. The threat from biological weapons has also become more diverse as biological weapon agents can be employed in a variety of ways. The development of biological weapons is made easier by dual-use technologies. The following image demonstrates some of these attacks since 2013.[12]

Rapid advances in biotechnology, including gene editing, synthetic biology and neuroscience, will create new economic, military, ethical, and regulatory challenges worldwide as governments struggle to keep pace with these exponentially changing scenarios. These technologies hold great promise for advances in precision medicine, agriculture, and manufacturing. However, they also introduce risks, such as the potential for adversaries to develop novel biological warfare agents, threaten food security, and enhance or degrade human performance.

Biotechnologies, such as the low-cost gene-editing tool CRISPR-Cas9 have the potential to alter genes or create DNA to modify plants, animals, and humans. Such biotechnologies could be used to enhance (or degrade) the performance of military personnel. The proliferation of synthetic biology that is used to create genetic codes that do not exist in nature can be used to increase the number of actors able to create chemical and biological weapons. Adversaries may be less restrained in both researching and applying biotechnology, particularly as it relates to human performance modification and biological weapons.

■
12   United States Senate Intelligence Committee, 29 January 2019.

THE ELECTROMAGNETIC SPECTRUM

Penetrates Earth Atmosphere? Y | N | Y | N

Wavelength (meters): Radio | Microwave | Infrared | Visible | Ultraviolet | X-ray | Gamma Ray

10^3 | 10^{-2} | 10^{-5} | $.5 \times 10^{-6}$ | 10^{-8} | 10^{-10} | 10^{-12}

About the size of... Buildings | Humans | Honey Bee | Pinpoint | Protozoans | Molecules | Atoms | Atomic Nuclei

Frequency (Hz): 10^4 | 10^8 | 10^{12} | 10^{15} | 10^{16} | 10^{18} | 10^{20}

Temperature of bodies emitting the wavelength (K): 1 K | 100 K | 10,000 K | 10 Million K
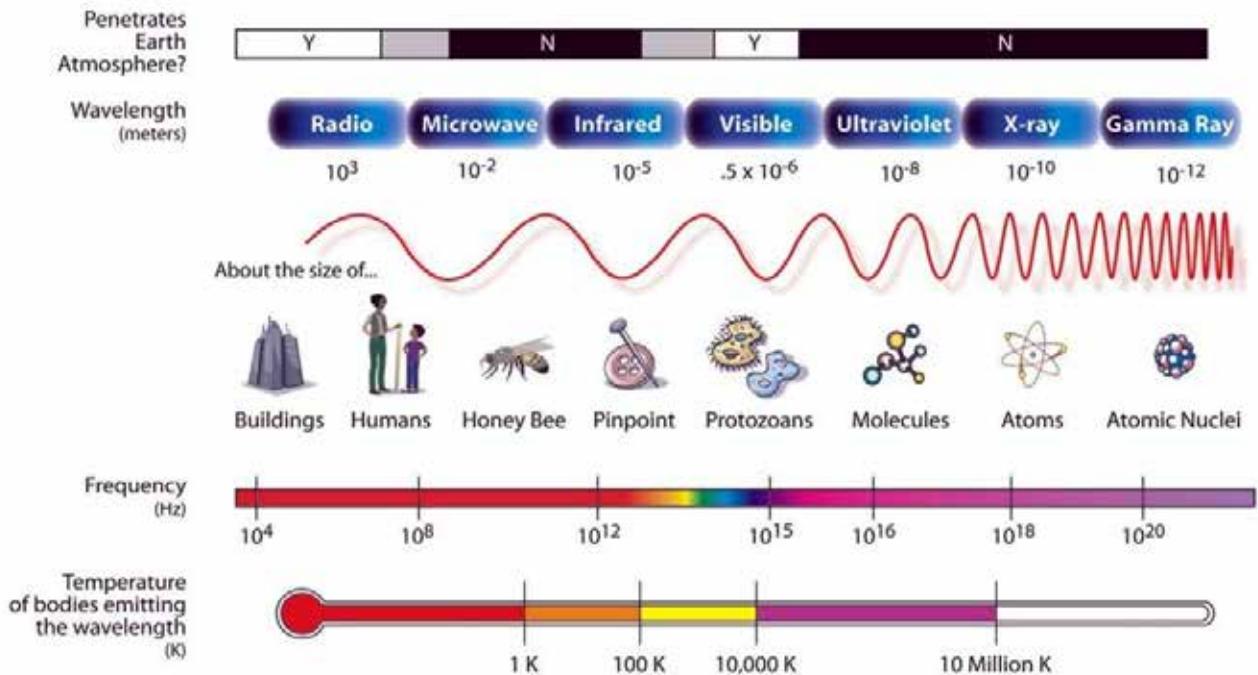
■ Table: The electromagnetic spectrum spans radio waves to gamma waves. Credit: NASA

Directed energy and hypersonic weapons

The recent growth and development of electromagnetic weapons is attributed to defense against terrorist attacks, chemical, biological, radiological, and nuclear materials for the purpose of national security and protection of civilian. A directed-energy weapon (DEW) is a ranged weapon that damages its target with highly focused energy, including lasers, microwaves, particle beams, and sound beams.

Potential applications of this technology include weapons that target personnel, missiles, vehicles, and optical devices.

Scientists believe that U.S. embassies, personnel and diplomats around the world have been targeted with high-power microwaves.[13] The technology behind these weapons are not new. The latest episodes of so-called "Havana Syndrome" took place in Berlin. The U.S. embassy has handed over evidence of this attack to authorities in Germany for investigation.[14] The first reported cases date back to 2016 in Havana, however these cases go back for many years. Physicians, scientists, and government officials have been trying to find out what causes the "Havana Syndrome". The electromagnetic weapon market is

■

13   The Conversation, 2020, Retrieved in 2021, https://theconversation.com/scientists-suggest-us-embassies-were-hit-with-high-power-microwaves-heres-how-the-weapons-work-151730

14   Germany investigates possible 'sonic weapon attack' against US embassy staff, the Guardian, https://www.theguardian.com/world/2021/oct/08/germany-havana-syndrome-sonic-weapon-us-embassy-staff

125

anticipated to grow exponentially in the emerging technology market. This technology is cheap and easy to use with high precision for targets in any setting.

Cyberspace

Conflicts between states are taking place in space through cyber operations and attacks. Cyberspace has become a critical security concern for all governments around the world. This concern has grown exponentially over the years and the COVID-19 pandemic has exacerbated relevant vulnerabilities. Denial of service or destructive malware, cyber espionage or intelligence activity and breach of confidentiality of data are some examples of cyberattacks. Global access to space services has expanded for civil, commercial, intelligence, and military purposes, in part because of technological innovations, private-sector investments, international partnerships, and the demand from emerging markets. Foreign governments will continue efforts to expand their use of space-based reconnaissance, communications, and navigation systems - including by increasing the number of satellites, quality of capabilities, and applications for use.

Cyber attacks can disrupt Chemical, Biological, Radio-logical and Nuclear (CBRN) facilities. Such facilities are automated and run by computers that are connected to larger networks that can be compromised. When these facilities are penetrated through cyber-attacks the facilities themselves can become the equivalent of weapons of mass destruction themselves. These potential threats are near impossible to predict. Terrorist organizations want to acquire CBRN material which poses a major threat for the international community. The cyber domain is considered as major international security risks. More attention needs to be paid to terrorist activities online. Two prominent areas that terrorist organizations and groups have had much success with are communication of their propaganda and their recruitment efforts.[15]

The rise of a GPS society and the decline of human intelligence

Conflicts between states are taking place in space through cyber operations and attacks. Cyberspace has become a critical security concern for all governments around the world. This concern has grown exponentially over the years and the COVID-19 pandemic has exacerbated rele-

> **Is this the future we want for humanity? Do we want to let emerging technologies such as AI to make decisions for us?**
>
> "

15   Nasheri, H. Economic Espionage and Industrial Spying, Cambridge University Press, New York, London, 2005, 270 pp.

vant vulnerabilities. Denial of service or destructive malware, cyber espionage or intelligence activity and breach of confidentiality of data are some examples of cyberattacks. Global access to space services has expanded for civil, commercial, intelligence, and military purposes, in part because of technological innovations, private-sector investments, international partnerships, and the demand from emerging markets. Foreign governments will continue efforts to expand their use of space-based reconnaissance, communications, and navigation systems - including by increasing the number of satellites, quality of capabilities, and applications for use.

Cyber attacks can disrupt Chemical, Biological, Radiological and Nuclear (CBRN) facilities. Such facilities are automated and run by computers that are connected to larger networks that can be compromised. When these facilities are penetrated through cyber-attacks the facilities themselves can become the equivalent of weapons of mass destruction themselves. These potential threats are near impossible to predict. Terrorist organizations want to acquire CBRN material which poses a major threat for the international community. The cyber domain is considered as major international security risks. More attention needs to be paid to terrorist activities online. Two prominent areas that terrorist organizations and groups have had much success with are communication of their propaganda and their recruitment efforts.[16]

THE AUTHOR

Hedi Nasheri is a Professor of Criminology and Justice Studies and the Director of Graduate Program in Criminology in the Department of Sociology at Kent State University in the United States. She is a Visiting Professor in the Faculty of Law at the University of Turku in Finland. Professor Nasheri's academic research and teaching, as well as her practical experience, has focused for a number of years on issues related to cybersecurity and technology crimes, intelligence and national security and transnational crimes as it relates to global security. She has collaborated throughout the years with members of the Intellectual Property Section of the Department of Justice and members from the Federal Bureau of Investigation Counterterrorism Section on a number of educational and research presentations domestically and internationally for a broad range audience including, the private sector, law enforcement and academia. More recently, she was appointed as Senior Fellow to the Policy Division of the Business Executives for National Security (BENS). Her work at BENS addressed the relationship of theft of sensitive and propriety information and its risk to U.S. national security.

16   Nasheri, H. Economic Espionage and Industrial Spying, Cambridge University Press, New York, London, 2005, 270 pp.

INFOCUS

by Brooke Ellison

COVID-19 AND THE EROSION OF DISABILITY RIGHTS

Introduction

The historical lore that will be crafted around the COVID-19 pandemic will be a tale of social inequalities. However, while the existence of social inequalities is well documented and have characterized societies for centuries, the COVID-19 pandemic, like many other societal catastrophes before, has made visible, tangible, and measurable how these social inequalities have real and consequential impacts on the lives of marginalized people. There is perhaps no demographic group that has felt the slings and arrows of societal injustice more acutely than people with disabilities throughout the pandemic. At every phase of the COVID-19 pandemic, people with disabilities have disproportionately experienced its cruelty. And, yet, like all seminal moments in history, our slow but collective reemergence from the pandemic provides a pristine opportunity to learn. The pandemic brought some of our most gaping societal fault-lines into stark relief, and we need to use this time of increased clarity to better understand the multitudinal ways that people with disabilities are denied many of the

> **At every phase of the COVID-19 pandemic, people with disabilities have disproportionately experienced its cruelty**

basic freedoms that others enjoy and how these denials have immeasurable – even fatal – impacts on their lives.

Disproportionate disease Burden

The COVID-19 pandemic has taken a nearly unfathomable human toll. However, the enormity of the death toll associated with COVID-19 among the general population, drastically underestimates the death toll among people with disabilities. As the U.S. Centers for Disease Control And Prevention (CDC) has studied extensively and articulated, people with underlying medical conditions were at a much higher risk of experiencing severe outcomes from Covid 19. Severe outcomes are characterized by hospitalizations, admissions to intensive care units (ICU), intubation or mechanical ventilation, or death. According to one study, the underlying medical conditions known to put people at greater risk include history of myocardial infarction, cerebrovascular disease, congestive heart failure, dementia, diabetes, chronic pulmonary disease, and hyperlipidemia (1). Many people who live with a physical disability, are predisposed to many of the comorbidities that also increase the likelihood of severe outcome if infected with COVID-19. (2). While this is known, quantifiably, to be the case, a true "health disparity" implies the presence of an unnecessary inequality among

different populations with respect to the burden and risk of experiencing healthcare challenges. We should ask ourselves "Why is it that people with disabilities suffer higher rates of the conditions that put one at greater risk to die from COVID-19?" The answer to this question gets to the very heart of the human rights abuses and historical disadvantages that people with disabilities have, likewise, encountered.

Sociocultural factors

Article 25 of the UN Convention on the Rights of Persons with Disabilities (CRPD) was drafted to ensure the rights of people with disabilities to receive the highest standard of healthcare, without discrimination (3). Article 25 states, "Persons with disabilities have the right to the enjoyment of the highest attainable standard of health without discrimination on the basis of disability." While 164 countries have signed the convention, and 182 countries have ratified the CRPD (4), the actual care and services that people with disabilities receive are far from adequate. While this fact, in itself, is a social injustice in need of remedy, as Dickinson and Kavanagh have argued, health inequalities only worsen during epidemics and pandemics. The fact is that marginalized communities have fewer resources available to them and struggle to access the basic supplies and services needed for survival. This confluence of predisposition to underlying conditions, inadequate access to primary healthcare, and marginalization from needed social supports and services has put people with disabilities in a dangerous, yet avoidable situation.

It is not only comorbidities that have affected the disproportionality with which people with disabilities have acquired COVID-19, but so, too, have the logistical needs that their lives demand. Successful combat of the SARS-CoV-2 virus is contingent upon strategic decisions and planning. Yet, as it has become clear very early on, many of the planned measures designed to respond to and control the pandemic failed to include people with disabilities. For instance, COVID-19 exposed the existing lack of health information accessible for people with disabilities. In an article published by Dror and colleagues, the authors explored the accessibility of web-based health information provided by countries

■ © UNDP Bangladesh 2020 COVID19 distribution

around the world (5). The researchers found that, upon investigating websites from the health authorities of 189 countries, only 4.7% had fully implemented the Web Accessibility Initiative access guidelines. This, as the authors argue, prevents millions of disabled people from acquiring the information they need to stay safe during the pandemic.

The disproportionate burden that people with disabilities have experienced during the pandemic can be seen, most visibly, in the sheer numbers: the unimaginable numbers of people with disabilities who perished from the virus. While one in 15 people live with a disability, according to the 'UK's Office of National Statistics, six out of ten COVID-19 related deaths were among people with disabilities (6). These data were accumulated

> **Upon investigating websites from the health authorities of 189 countries, only 4.7% had fully implemented the Web Accessibility Initiative access guidelines**

in a developed nation-state, but it is arguable that they are much more exaggerated in developing nations, where an estimated 80% of people with disabilities live and where there are far fewer resources available (7). From this standpoint, people with disabilities have been multiplicatively disadvantaged throughout this pandemic, dying at far higher rates than the general population. They are, being denied access to pandemic planning protocols and information, and disproportionately live in the countries least-able to provide resources to people who require additional social supports.

Long-Term-Care confinement

While COVID-19 strained the entire global healthcare system, the residents in long-term care facilities (LTCs) were the ones who experienced the most devastating impacts of the pandemic. According to data compiled by the Kaiser Family Foundation (KFF), within the United States alone, 1.3 million individuals with disabilities live in nursing homes, 800,000 live in assisted living facilities, and 75,000 live in intermediate care facilities. As the data collected by KFF very early in the pandemic showed, by April 2020 more than 10,000 deaths due to COVID-19 in long term care facilities, representing 27% of the deaths due to the pan-

demic in the US. By November 2020, that number had jumped to 100,000 deaths among LTC residents and staff. Likewise, the data collected by KFF demonstrated that, within six U.S. states, over 50% of all COVID-19 deaths were among long-term care residents with disabilities (8). These data were true, even though people with disabilities living in long-term care facilities account for less than 1% of the US population.

Given the findings of much research, it has been clear that the COVID-19 pandemic took a disproportionate toll on residents of long-term care facilities, with this population accounted for some 38% of COVID deaths. While residents of long-term care facilities are undeniably among the sickest members of the collective population, it is not solely for this reason that they were the most vulnerable. The structure and operation of LTCs are less akin to those of healthcare settings like hospitals than they are to other institutionalized organizations like prisons. The later are characterized by high person-density - higher density is incentivized - and little opportunity for physical distancing; while autonomous decision-making is essentially nonexistent. As physician and researcher Cynthia Holzer argued (9), the routines embedded within American long-term care facilities, in particular, are organized "for

the efficient operation of the facility, rather than the needs of the residents" (p. 205). The business model implemented in many long-term care facilities has fostered a particularly high turnover rate among long-term care staff, which can be as high as between 70% and 100% turnover per year. In a time like a pandemic that, as mentioned, has been spread through staff-spread infection, this high turnover rate is especially consequential.

Not only were people with disabilities living in nursing homes more at risk of becoming infected with COVID-19 due to the structure of these facilities, and dying from the virus because of their propensity to have underlying health conditions, but they also suffered from isolation. Soon into the pandemic, healthcare facilities of all kinds discontinued visitation rights for family members. Loved ones, who would otherwise visit their friends and family members in nursing homes, were denied access to do so due to the risk of bringing in infection. Disabled residents of these institutions were denied all access to the very people who had historically provided love, protection, comfort, and meaning for their lives. The ongoing consequences of this situation are still felt to this day.

> **Disabled residents of these institutions were denied all access to the very people who had historically provided love, protection, comfort, and meaning for their lives**

A report issued in March 2021 by Human Rights Watch assessed the ongoing effects of the nursing home visitation restrictions on their residents' physical and mental health (10). Based on data obtained from interviews and reports from stakeholders in the field, the report revealed instances of "extreme weight loss, dehydration, untreated bedsores, inadequate hygiene, mental and physical decline, and inappropriate use of psychotropic medications among nursing home residents." (10). Failures to ensure sufficient nursing homes staff, and to adequately regulate these facilities, reduced the ability to provide sufficient and consistent support to nursing home residents when they most needed it. Not only was support and care inadequate when other residents were dying at an incalculable rate, but also there were no loved one to provide the care, support, and love they so desperately needed. In addition, as the Human Rights Watch report stated, family members and independent monitors, who were unable to visit facilities throughout the pandemic, would often help ensure the adequacy of care and transparency, both of which faltered during the pandemic. Thus, the sense of longing, the feelings of isolation, and the measurable erosion of quality care experienced by people with disabilities living in long-term care facilities have had a disastrous effect.

Sociocultural factors

The disproportionate toll that the COVID-19 pandemic took on people living with disabilities in terms of cases and deaths is an injustice, but it has been well-established in the media. Likewise, the risk of people with disabilities living in long-term care facilities during the pandemic has been the focus of much social criticism. However, in addition to these direct disparities, people with disabilities suffered disproportionately in sociocultural ways throughout the pandemic, as they have through a somewhat perverse twist of fate in disasters of many kinds. (11). In these instances, it would be unfair and inadequate to presume that the disproportionate impact that disasters of any kind, pandemics included, have on people with disabilities is solely related to a degree of physical vulnerability. Rather, there are structural biases and sociodemographic inequalities experienced by people with disabilities that exacerbate the impact that a disaster brings about, affecting a broad variety of human rights issues that have historically challenged the lives of people with disabilities. Some of the rights concerned relate to access to adequate healthcare, access to housing, opportunities for employment, involvement in education, access to transportation and infrastructure, and their subjection to poverty. Until these matters are addressed, people with disabilities will chronically bear a disproportionate burden in times of disaster.

As we have seen during the COVID-19 pandemic, access to needed services can be difficult to acquire. Many people with disabilities require daily care and support services from external service providers in order to live their lives, and none of these needs stops during the time of a disaster like COVID-19, as Kendall has written. While measures like physical distancing were required to slow the spread of COVID-19, many people with disabilities were either unable to physically distance from service providers who could carry the virus or, conversely, did not have access

to the services they required because the services had to be discontinued. Both of these extremes put their lives at risk. Equipment and medical supplies, including respiratory care supplies like oxygen and ventilator tubing, remain essential for the lives of people with disabilities who require them yet, as was documented many times throughout the pandemic, access to these supplies was regularly inadequate, and much of the supply in existence was routed to clinical healthcare settings. In addition, during a pandemic like COVID-19, healthcare workers, who many people with disabilities rely on for care, can be redeployed to seemingly more immediate locations, like hospitals. The need for healthcare resources is a constant in the lives of many people with disabilities. Yet, during the COV-

ID pandemic, these resources were stretched thin - nearly to the point of depletion - leaving people with disabilities without access to supplies and services on which their lives depend. While some people with disabilities went without needed supplies while others, who had the financial means to do so, spent thousands of dollars to veritably stockpile medical supplies so as to avoid an inability to receive them.

Triaging of care

The centrality of the human rights challenges experienced by people with disabilities throughout the COVID-19 pandemic lies in the old-fashioned yet persistent notion that the lives of people with disabilities are less valuable than the lives of people without disabilities. That erroneous belief has sat at

the cornerstone of many disproportionate burdens that people with disabilities have borne during various types of disasters: the Fukushima nuclear power plant disaster - in which people with disabilities had a mortality rate twice that of those without - and the Hurricane Katrina, in which 38% of those who were not evacuated from the floods were people with disabilities (12). The perceived relative worth of people with disabilities has played no small role in the overall impact of the COVID-19 pandemic on the lives of this population, and this has been made manifest in many of the most gut-wrenching circumstances that the pandemic has created.

The coronavirus pandemic has exposed many vulnerabilities within our healthcare

135

system, and central among these is the lack of access to resources needed to provide adequate and safe medical care. We have seen these distributive injustices represented across many resources, including access to Personal Protective Equipment (PPE), hospital beds, medication and even healthcare personnel, and the provision of lifesaving and life-sustaining technology. Throughout the months of this pandemic, and even in years preceding it, ethicists, policymakers and philosophical thinkers have given attention to how the radical shifts in the demand for healthcare, like that brought about by the COVID-19 pandemic, would influence the metrics by which scarce healthcare resources are allocated and how care is triaged. This conundrum has consistently put people with disabilities in crosshairs.

Among the many concerns that people with disabilities have had to navigate during the pandemic has been what is called the U.S. "critical care

The perceived relative worth of people with disabilities has played no small role in the overall impact of the COVID-19 pandemic on the lives of this population
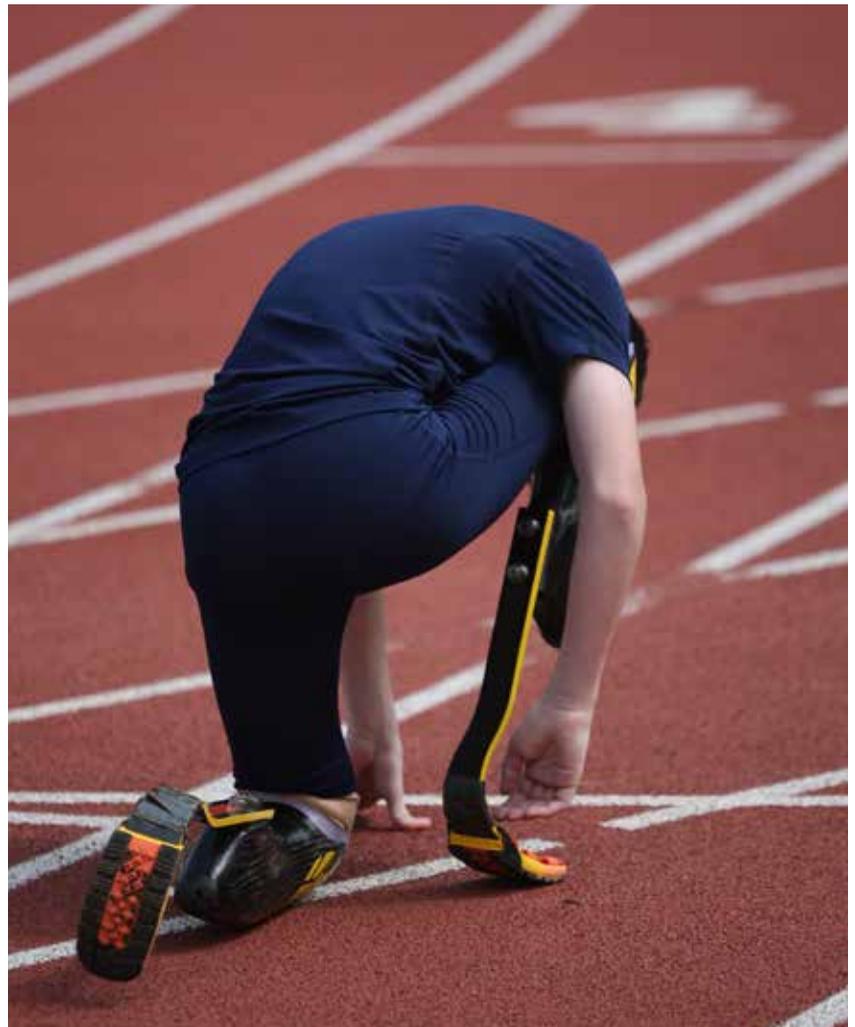
crisis triage protocols." These protocols provide guidance to hospitals and healthcare providers on how to distribute care when the number of people in need of support exceeds the capacities to meet their needs. The crisis care protocols in place throughout the pandemic were used as a framework for allocating healthcare resources. In other words, the system that determines who receives care over others – was based on a series of relatively subjective criteria, including a patient's anticipated or demonstrated resource-intensity needs, the relative survival possibilities of patients deemed likely to benefit from medical treatment, and assessments of pre-or post-treatment quality-of-life. (12) The concepts of "anticipated or demonstrated resource-intensity needs" and "perceived quality-of-life" have consistently put people with disabilities in an unsafe situation concerning the prioritization of their lives. The nature of many people with disabilities lives is such that they are complex and require resources. In other words, they are resource-intense, through no fault of their own. Yet, they are valuable; they are far more valuable than the undervalued way they have been represented in history, in media, by philosophical thinkers, and even by people like physicians and ethicists who have notoriously undervalued the quality of life for people with

> **Fairness and justice are not identical concepts, in the same way, that treating people equally does not imply equal outcomes when people begin at different starting points**

disabilities. They have failed to appreciate their value despite the intensity of resources that people with disabilities might need to lead meaningful lives. According to a study done at the University of Georgia, throughout the COVID-19 pandemic, unconscious biases within the healthcare system influenced how individuals with intellectual disabilities were prioritized in emergency triage protocols, such that able-project patients were frequently provided resources over people with intellectual disabilities. The argument was made that these individuals were poor candidates for life support, an unfounded claim. In other circumstances, equally devastating, adults with disabilities have been prevented from having visitors or advocates accompany them to the hospital throughout the pandemic. In some cases, these individuals are

unable to communicate their needs, and this puts them at high risk for abuse or denial of treatment. (13)

The bioethical concept of managing how scarce resources should be allocated is known as "distributive justice", which argues for a fair process. However, fairness and justice are not identical concepts, in the same way, that treating people equally does not imply equal outcomes when people begin at different starting points, and the disproportionality with which pandemics victimizes people with disabilities. Making "fairness" far less relevant than justice. Particularly in the event of this COVID-19 pandemic, which preys upon those with weakened bodies, people with disabilities are already at increased peril. This disease is discriminatory against people who experience physical problems. For people with disabilities, their bodies have already failed them, and we, as a society, cannot fail them as well.

Access to vaccines

The disadvantages experienced by people with disabilities throughout the pandemic have continued since the development and distribution of vaccines. Despite the fact that many allocation structures for the distribution of vaccines prioritized people with underlying healthcare conditions,

many of whom were people with disabilities, the ability for this population to, in actuality, receive that vaccine has been muddled and complex. According to disability activists and advocacy organizations around the world, throughout the pandemic and continuing into the vaccination phase, people with disabilities have been left behind, as activists in Canada had argued (14). A similar argument was made by health department officials in Australia, who stated that two months into the vaccination efforts, only 6.5% of people with disabilities had been vaccinated, despite the fact that this population was prioritized in the vaccine rollout.(15) The sentiment felt by many people with disabilities is not unfounded, as not only

have the vaccination protocolsbeen challenging for this population but so, too, have the attempts to navigate the existing structural barriers that people with disabilities face when navigating daily life.

Particularly during the early phases of the vaccination rollout, securing an appointment for a vaccine was extremely difficult. It required access to online web portals or repeated phone calls to Departments of Health. For many people with disabilities, these platforms are inaccessible. This level of inaccessibility prevented members of this population from securing vaccine appointments, despite their eligibility for them. In addition, as vaccination sites were created with the general population in mind, not all

vaccination sites have been accessible for wheelchair users or people with disabilities. Until the very recent integration of mobile vaccination units and advocacy efforts to ensure that vaccination sites are fully accessible, people with disabilities have been without options. And, these logistical challenges accompany the existing structural barriers that people with disabilities encounter in their daily lives, such as a lack of accessible transportation or support persons to assist when attending the vaccine appointment. Finally, for many people with disabilities, leaving their homes or even their beds is either a challenge or an impossibility, veritably removing this entire population from access to the vaccine.

In addition to the logistical barriers that people with disabilities have faced within the terms of getting vaccinated, there have been many concerns regarding how their unique bodies might be affected by that vaccine. As is the case with many marginalized groups, people with disabilities have been largely excluded from the clinical trials that demonstrate the safety and efficacy of medical interventions, including the COVID-19 vaccines. As has been well documented, there has been skepticism and hesitance among the general population about the safety of the COVID-19 vaccine. Preliminary data collected among people with disabilities on this same issue, though, have demonstrated levels of skepticism or concern at or above those found in the general population. For instance, according to a survey conducted with people living with spinal cord injury, 72% of respondents who had already received the COVID-19 vaccine had concerns about it. (16) Similarly the same study, also shows that only about 60% of respondents said they had enough information about the safety of the vaccine for people with spinal cord injury. Many were concerned about the lack of resources, outreach efforts, and information dissemination provided to people living with this condition. The existing trauma to and strain on their bodies might put them at higher risk for complications from the vaccine. While it is quite possible that these concerns do not reflect the accuracy of available scientific and clinical data regarding vaccines and their effect on people with disabilities like spinal cord injury, what is quite clear is that people with disabilities are not receiving the information and reassurance they need to feel comfortable receiving the vaccine.

Opportunity to rebuild

As the global population ages and as we see the ongoing effects of the COVID-19 pandemic on physical and mental health, the number of people worldwide with a disability will see a significant increase. This is not a tragedy. It is an opportunity. People with disabilities are human beings, fully deserving of the full spectrum of human rights. Disability rights are human rights. And, yet, for far too long, people with disabilities have historically been viewed as less worthy, less valuable, and less deserving of our concern than are those without disabilities. This has been seen repeatedly, in the level of disregard they are afforded during times of disaster, in the ways that nations and economies have been built and developed. This either objectify their bodies, quantify their relative lack of productivity or marginalizes

> **Not all vaccination sites have been accessible for wheelchair users or people with disabilities**

their existence so that their social participation is either discouraged or denied. Concepts like the quality adjusted life year (QALY) or the disability adjusted life year (DALY), thatcalculate a country's Global Burden of Disease through the estimate of the number of years of healthy life lost due to living with a disability, have been used by international organizations like the World Bank in international development initiatives for the creation of public policy creation. Central to these concepts is the notion that a life lived with a disability is some inferior or less desirable state: that which degrades or erodes some other, more optimal state of existence. Until that interpretation of disability changes, and until the world stops seeing disability as a detriment or net negative, people with disabilities will continually find themselves in a position of disadvantage or multiplicative discrimination whenever disasters arise or distribute different decisions must be made.

139

However, in the coming months and years, as the world begins to awaken from the oppression generated by the pandemic, and begin to rebuild itself, it will also have the opportunity to reconstruct society more equitably. It gives us the chance to reimagine the respect it affords to diverse ways of life and rebuild our communities and policies in a more just way. Policies that allow people with disabilities to live at home, in their communities, rather than in long-term care facilities, must be included, as should the reconstruction of our healthcare system so that it is more accessible to people with diverse needs. This must include the reimagining of our infrastructure, our built environments, and our networks to be usable for everyone. Furthermore, policies that allow people with disabilities to emerge from conditions of poverty and become, to whatever degree they are able, contributing members of society, should also be included. And, most importantly, this must include deliberate and protracted efforts to reframe disability from a vision of vulnerability or societal detriment to one of empowerment and societal richness. People with disabilities must be provided with opportunities, not just to achieve the bare minimum but to thrive and excel and demonstrate their worth, no matter what their level of achievement might be. This is our opportunity. Emerging from the pandemic in the years ahead, this is our chance to set policies straight, to promote inclusion for everyone, and to approach the future – whatever challenges it may bring – in a safer, more secure, more sustainable, and more inclusive way.

THE AUTHOR

Brooke Ellison, PhD is an Associate Professor at Stony Brook University, studying medical ethics and health policy. Dr. Ellison received her undergraduate degree in cognitive neuroscience from Harvard University in 2000, followed by her Master Degree in Public Policy from the Harvard Kennedy School in 2004. After running for New York State Senate in 2006, Dr. Ellison completed her PhD in Sociology from Stony Brook University in 2012. Dr. Ellison has lived with a physical disability for 30 years. In these decades, Dr. Ellison has understood firsthand the challenges and social deficits that disability can create but, also, how these challenges and deficits can be alleviated through technological innovation, social supports, and policy measures.

REFERENCES

1. Prevention, Centers For Disease Control and. Underlying Medical Conditions Associated with High Risk for Severe Covid-19: Information for Healthcare Providers. *www.cdc.gov.* [Online] March 29, 2021. [Cited: April 20, 2021.] https://www.cdc.gov/coronavirus/2019-ncov/hcp/clinical-care/underlyingconditions.html#print.

2. Dickinson, H and Kavanagh, A. People with a disability are more likely to die from coronavirus – but we can reduce this risk. *Medical Express.* [Online] March 20, 2020. [Cited: April 19, 2021.]

3. Disability, United Nations Department of Economic and Social Affairs. *Article 25 – Health.* s.l.: United Nations: Department of Economic and Social Affairs, disability, 2006.

4. Convention on the rights of persons with disabilities (CRPD). United Nations Department of Economic and Social Affairs, Disability. [Online] October 2006. [Cited: April 20, 2021.] https://www.un.org/development/desa/disabilities/convention-on-the-rights-of-persons-with-disabilities.html.

5. A lesson from COVID-19 on inaccessibility of web-based information for disabled populations worldwide. Dror, AA, et al. s.l.: bioRxiv, 2020.

6. Statistics, Office of National. Updated estimates of coronavirus (COVID-19) related deaths by disability status, England: 24 January to 20 November 2020. London : s.n., 2020.

7. Affairs, United Nations Department of Economic and Social. Fact sheet on persons with disabilities. Geneva, Switzerland: s.n., 2020.

8. Chidambaram, Priya. State reporting of cases and deaths due to COVID-19 in long-term care facilities. s.l.: Kaiser Family Foundation, 2020.

9. culture change in long-term care. Holzer, C. 7, Rhode Island: Medicine and Health, 2007, Vol. 90.

10. Watch, Human Rights. US: concerns of neglect in nursing homes. 2021.

11. Immediate and long-term implications of the COVID-19 pandemic for people with disabilities. Kendall, E, et al. 12, s.l. : American Journal of Public Health, 2020, Vol. 110.

12. Covid-19 Crisis Triage – Optimizing Health Outcomes and Disability Rights. Solomon, M, Wynia, MK and Gostin, L. 5, s.l. : New England Journal of Medicine, 2020, Vol. 383.

13. Discrimination and bias in state triage protocols towards persons with intellectual disabilities during the COVID-19 pandemic. Felt, AB. s.l. : Disaster and Public Health Preparedness, 2021.

14. Kennedy, Brendan. People with disabilities face confusion and other barriers to getting COVID-19 vaccines. A task force is working to change that. Toronto Star. 2021.

15. Knaus, C. Australians with a disability "forgotten" in coronavirus vaccine rollout, advocates say. The Guardian. 2021.

16. Stone, J. COVID-19 vaccine and people with spinal cord injuries. Forbes. 2021.
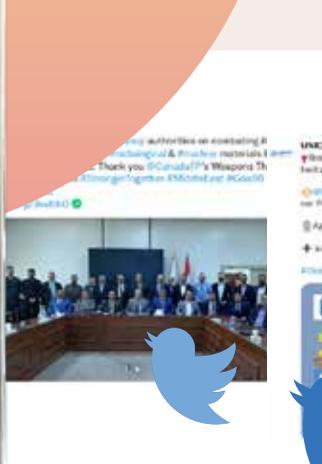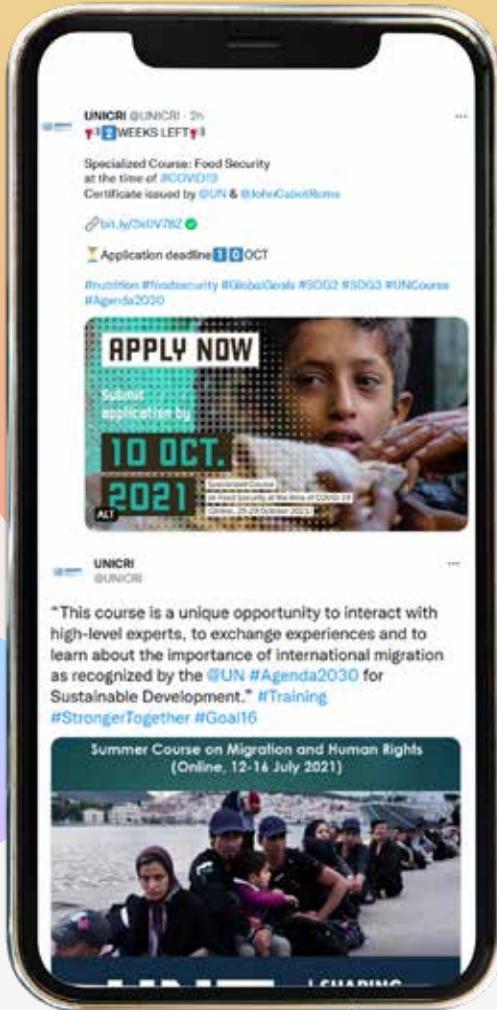
Follow **UNICRI** on [Twitter](#)
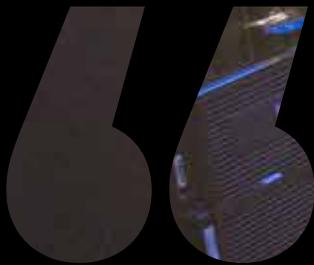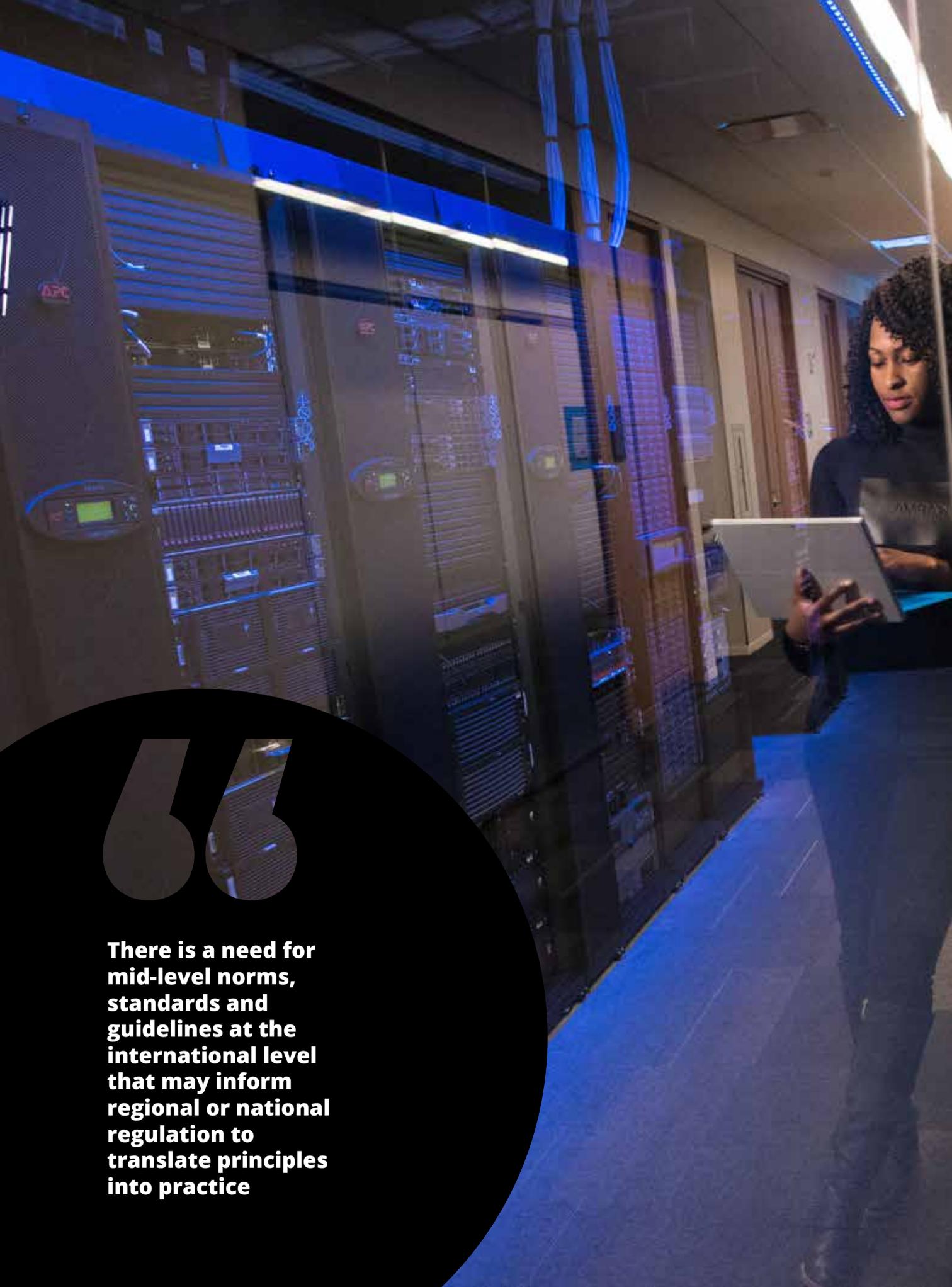
There is a need for mid-level norms, standards and guidelines at the international level that may inform regional or national regulation to translate principles into practice

INFOCUS

by Prateek Sibal

RISK-BASED APPROACHES TO ARTIFICIAL INTELLIGENCE (AI) GOVERNANCE

Recent advancements in AI technologies leading to new commercial applications with potentially adverse social implications: the way forward

Over the last five years, 117 initiatives worldwide have published Artificial Intelligence (AI) ethics principles. Despite a skewed geographical scope (91 of these initiatives come from Europe and North America), the proliferation of such initiatives on AI ethics principles is paving the way for building global consensus on AI governance. Notably, the 38 OECD Member States have adopted the OECD AI Recommendation, the G20 has endorsed these principles, and the Global Partnership on AI is operationalising them. UNESCO is furthermore developing a Recommendation on the Ethics of AI that 193 countries may adopt in 2021.

An analysis of different principles revealed a high-level consensus around eight themes: (1) privacy, (2) accountability, (3) safety and security, (4) transparency and explainability, (5) fairness and non-discrimination, (6) human control of technology, (7) professional responsibility, and (8) the promotion of human values. However, these

ethical principles are [criticised](#) for lacking enforcement mechanisms. Companies often commit to AI ethics principles to improve their public image yet give little follow-up on implementing them, an exercise termed as «[ethics washing](#)». Evidence also [suggests](#) that knowledge of ethical tenets has little or no effect on whether software engineers factor ethics into the development of their products or services.

Defining principles is certainly essential, but it is only a first step to developing ethical AI governance. There is a need for mid-level norms, standards and guidelines at the international level that may inform regional or national regulation to translate principles into practice. This article discusses the need for AI governance to evolve past the "ethics formation" stage by implementing concrete and tangible steps, such as developing technical benchmarks and adopting risk-based regulation.

Recent Advances in AI Technologies

Artificial Intelligence is developing rapidly. The 2021 AI Index report notes four crucial technical advances that hastened the commercialisation of AI technologies:

▶ AI-Generated Content: AI systems can generate high-quality text, audio and visual content to a level that it is difficult for humans to distinguish between synthetic and non-synthetic content.

▶ Image Processing: Computer vision has seen immense progress in the past decade and is fast industrialising in applications that include autonomous vehicles.

▶ Language Processing: Natural Language Processing (NLP) has advanced such that AI systems with language capabilities now have economic value through live translations, captioning, and virtual voice assistants.

▶ Healthcare and biology: DeepMind's AlphaFold solved the decades-old protein folding problem using machine learning techniques.

"

There is a need for mid-level norms, standards and guidelines at the international level that may inform regional or national regulation to translate principles into practice

These technological advances have social implications as well as economic value. For instance, the technology generating synthetic faces has rapidly improved. As shown in Figure 1, in 2014, AI systems produced grainy faces, but by 2017, they were generating realistic synthetic faces. Such AI systems have led to the proliferation of 'deepfake' pornography that overwhelmingly targets women and has the potential to erode people's trust in the information and videos they encounter online. Some actors misuse the deepfake technology to spread online disinformation, resulting in adverse implications for democracy and political stability. Such developments have made AI governance a pressing matter.

Challenges of AI Governance

These rapid advancements in the field of AI technologies have brought the need for better governance to the forefront. In thinking about AI governance, any [governments](#) worldwide are concerned with enacting regulation that does not stifle innovation yet also provides adequate safeguards to protect human rights and fundamental freedoms.

Technology regulation is complicated because, until a technology has been extensively developed and widely

used, its impact on society is difficult to predict. However, once a technology is deeply entrenched and its effect on society is understood better, it becomes more challenging to regulate. This tension between providing free and unimpeded technology development while regulating adverse implications is termed the "Collingridge dilemma".

David Collingridge, the author of the Social Control of Technologies, notes that when regulatory decisions have to be made before a technology's social impact is known, continuous monitoring can help mitigate unexpected consequences. Collingridge's guidelines for decision-making under ignorance can inform AI governance as well. These include choosing technology options with (1) low costs of failure, (2) short response times for responding to unanticipated problems, (3) low costs of remedying unintended errors, and (4) cost-effective and efficient monitoring.

Technical benchmarks for evaluating AI systems

Quantitative benchmarks are also necessary to address the ethical problems related to bias, discrimination, lack of transparency, and accountability in algorithmic decision-making. The Institute of Electrical and Electronics Engineers (IEEE), through its Global Initiative on Ethics of Autonomous and Intelligent Systems, is developing technical standards to address bias in AI systems. Similarly, in the United States, the National Institute of Standards and Technology (NIST) is developing standards for explainable AI based on principles that call for AI systems to provide reasons for their outputs in a manner that is understandable to individual users, explain the process used for generating the output, and deliver their decision only when the AI system is fully confident.

Going back to our previous example, there is already significant progress in introducing benchmarks for the regulation of facial recognition technology. Facial recognition systems have a large commercial market. They are used for various tasks, including law enforcement and border controls. These tasks involve detecting visa photos, matching photos in criminal databases, and detecting and removing child abuse images online.

However, facial recognition systems have been the cause of significant concern due to high error rates in detecting

Facial recognition systems have been the cause of significant concern due to high error rates in detecting faces and impinging on human rights

"

■ *Figure 1: Increasingly realistic synthetic faces generated by variations on Generative Adversarial Networks (GANs). In order, the images are from papers by Goodfellow et al. (2014), Radford et al. (2015), Liu and Tuzel (2016), and Karras et al. (2017)*

faces and impinging on human rights. Biases in such systems have adverse consequences for individuals, such as being [denied entry](#) at borders or being [wrongfully incarcerated](#). In the United States, the NIST's [Face Recognition Vendor Test](#) provides a benchmark to compare different commercially available facial recognition systems› [performance](#)s by operating their algorithms on different image datasets.

Defining benchmarks for ethical principles is an important step, however, in line with the Collingridge Dilemma, it needs to be complemented by risk assessments to mitigate adverse social impacts. Risk assessments would allow for the application of risk-proportionate AI regulation instead of a reliance on blanket rules that may hinder technological development with unnecessary compliance burdens. The next blog post in this two-part series will engage with some potential risk-based approaches to AI regulation.

AI Risk Assessment Frameworks

Risk assessments can help identify which AI systems need to be regulated. Risk is determined by the severity of the impact of a problem and the probability of its occurrence. For example, the risk profile of a facial recognition system to unlock a personal mobile phone would differ from a fa-

cial recognition system used by law enforcement. The former may be overall beneficial as it adds a privacy-protecting security feature. In contrast, the latter could have chilling implications on the freedom of expression and privacy. Therefore, the risk score for facial recognition systems is relative to their use and deployment context. The following are some of the approaches followed by various bodies in developing risk assessment frameworks for AI systems.

> **"**
>
> **Risk assessments would allow for the application of risk-proportionate AI regulation instead of a reliance on blanket rules**

The European Union (EU)

The European Commission's legislative proposal on Artificial Intelligence classifies AI systems by four levels of risk and outlines risk proportionate regulatory requirements. The categories proposed by the EU include:

1. Unacceptable Risk: The EC has proposed a ban on applications like social credit scoring systems and real-time

remote facial recognition systems in public spaces.

2. High Risk: AI systems that harm the safety or fundamental rights of people are categorised as high-risk. The proposal prescribes some mandatory requirements for high-risk AI systems.

3. Limited Risk: When the risks associated with the AI systems are limited, only transparency requirements are prescribed.

4. Minimal Risk: When the risk level is identified as minimal, there are no mandatory requirements, but the developers of such AI systems may voluntarily choose to follow industry standards.

Germany

In Germany, the Data Ethics Commission has proposed a five-layer criticality pyramid that requires no regulation at a low-risk level to a complete ban at high-risk levels (see Figure 2). The EU approach is similar to the German approach but differs in the number of levels.

The UK

The AI Barometer Report of the Centre for Data Ethics and Innovation identifies some common risks associated with AI systems and some sector-specific risks.

The common risks include:

1. Algorithmic bias and discrimination

2. Lack of explainability of AI systems

3. Regulatory capacity of the State

4. Breach in data privacy due to failure in user consent

5. Loss of public trust in institutions due to problematic AI and data use

The report identified that the severity of common risks varies across different sectors like criminal justice, financial services, health and social care; digital and social media; and energy and utilities. For example, algorithmic bias leading to discrimination is considered high-risk in criminal justice, financial services, health and social media but medium risk in energy and utilities. The risk assignment, in this case, was done through expert discussions. The UK's approach has a strong sector specific focus. The overall sector level risk is ascertained based on a combination of multiple AI risk criteria.

The Organisation for Economic Co-operation and Development (OECD)

The preliminary classification of AI systems developed by the OECD Network of Experts' working group on AI classification has four dimensions:

1. Context includes stakeholders that deploy an AI system, the stakeholders impacted by its use and the sector in which an AI system is deployed.

2. Data and inputs to an AI system influence the system›s outputs based on the data classifiers used, the source of the data, its structure, scale, and how it was collected.

3. The type of algorithms used in AI systems has implications for transparency, explainability, autonomy and privacy.

4. The kind of task to be performed and the type of output expected range from forecasting, content personalisation to detection and recognition of voice or images.

Applying this classification framework to different cases, from facial recognition systems and medical devices to autonomous vehicles, allows us to understand the risks under each dimension and design appropriate regulation. In autonomous vehicles, the context of transportation and its significant risk of accidents
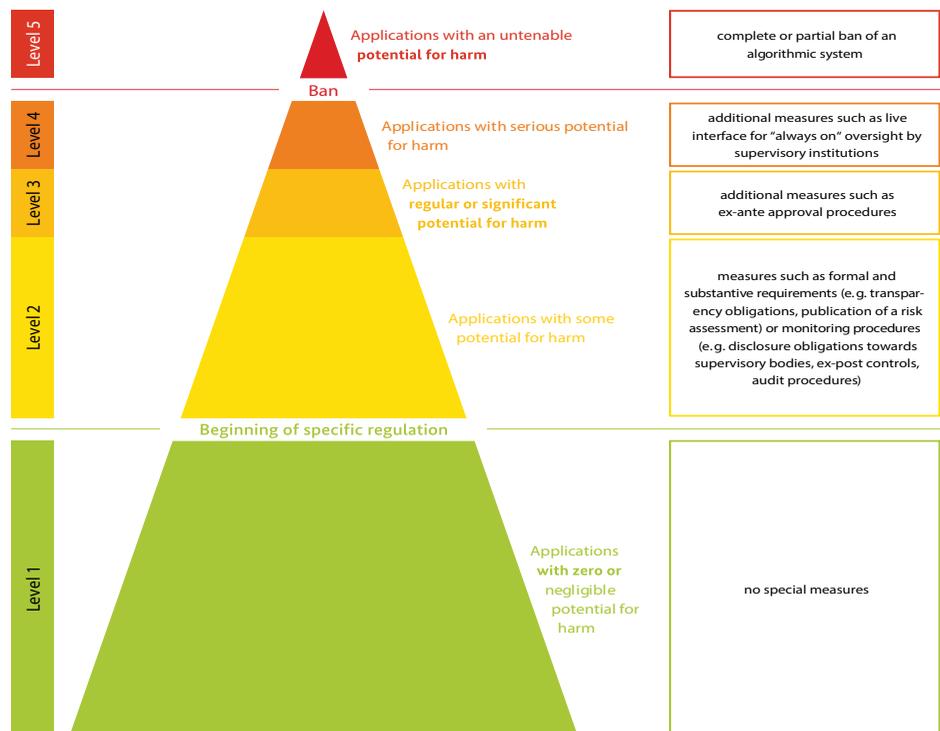
- Figure 2: Criticality pyramid and risk-adapted regulatory system for the use of algorithmic systems (Source: Opinion of the Data Ethics Commission)

Level 5 — Applications with an untenable **potential for harm** — complete or partial ban of an algorithmic system

Ban

Level 4 — Applications with serious potential for harm — additional measures such as live interface for "always on" oversight by supervisory institutions

Level 3 — Applications with **regular or significant potential for harm** — additional measures such as ex-ante approval procedures

Level 2 — Applications with some potential for harm — measures such as formal and substantive requirements (e. g. transparency obligations, publication of a risk assessment) or monitoring procedures (e. g. disclosure obligations towards supervisory bodies, ex-post controls, audit procedures)

Beginning of specific regulation

Level 1 — Applications with zero or negligible potential for harm — no special measures

increase the risk associated with its AI systems, and they are therefore considered a high-risk category requiring robust regulatory oversight.

Next steps in Risk-Adaptive Regulation for AI

The four approaches to risk assessment discussed above are systematic attempts to understand AI-related risks and develop a foundation for downstream regulation that can address risks without being overly prescriptive. With these examples in mind, national level initiatives could improve their AI governance by focusing on the following:

1. AI Benchmarking: AI systems need continuous development and updating of technical benchmarks to assess their performance under different contexts with respect to AI ethics principles.

2. Risk Assessments of AI applications: Risk assessments of AI systems require development of use cases of different AI applications under different combinations of contexts, data and inputs, AI models and outputs.

3. Systemic Risk Assessments: There is a need for systemic risk assessment in contexts where AI systems interact with one another. For example, in financial markets, different AI algorithms interact with

each other, and in certain situations, their interactions could cascade into a market crash.

Once AI risks are better understood, proportional regulatory approaches should be developed and subjected to Regulatory Impact Analysis (RIA). The OECD defines RIA as a "systemic approach to critically assessing the positive and negative effects of proposed and existing regulations and non-regulatory alternatives". RIAs can guide governments in understanding if the proposed regulations are effective and efficient in achieving the desired objective. Such impact assessments are good regulatory practice and will become increasingly relevant as more countries work towards developing their own national AI legislations.

Given the globalised nature of different AI services and products, countries should also develop their national level regulatory approaches to AI in conversation with one another. Importantly, these dialogues at the global and national level must be multi-stakeholder driven to ensure that different perspectives inform any ensuing regulation. Collectivised knowledge and coordination will lead to overall benefits by ensuring AI develops in a manner that is both ethically aligned and provides a stable environment for innovation and interoperability.

Once AI risks are better understood, proportional regulatory approaches should be developed and subjected to Regulatory Impact Analysis

THE AUTHOR

Prateek Sibal is a PhD Candidate in Governance and studies patterns of misinformation and disinformation on social media platforms in the context of political polarization. He is affiliated with the Centre for Digital Governance. He worked at the United Nations Educational, Scientific and Cultural Organisation's (UNESCO) on artificial intelligence and public policies for more than three years and is a lecturer on digital governance at the School of Public Affairs, Sciences Po, Paris. In the past he worked as a legislative analyst to a Member of Parliament in India. He has a Bachelor in Mechanical Engineering from VIT University, India and a Master in Public Policy (summa cum laude) from Sciences Po, Paris. His research interests include online communication, platform regulation, political polarization, media economics and digital governance.

THE POTENTIAL FOR DUAL-USE OF PROTEIN-FOLDING PREDICTION

by Sterling Sawaya, Taner Kuru, Thomas A. Campbell,

Artificial intelligence (AI) offers great potential for scientific advancement, particularly in areas with high complexity and many variables. Although biology can be challenging to comprehend, scientists can develop accurate AI models that help resolve biological interactions more effectively than conventional methods. Implementing AI in biological sciences promises benefits for all human beings by improving our understanding of how molecules interact or how genetic variation influences traits.

Traditional protein prediction methods rely on time-intensive methods requiring expensive equipment. Unfortu-
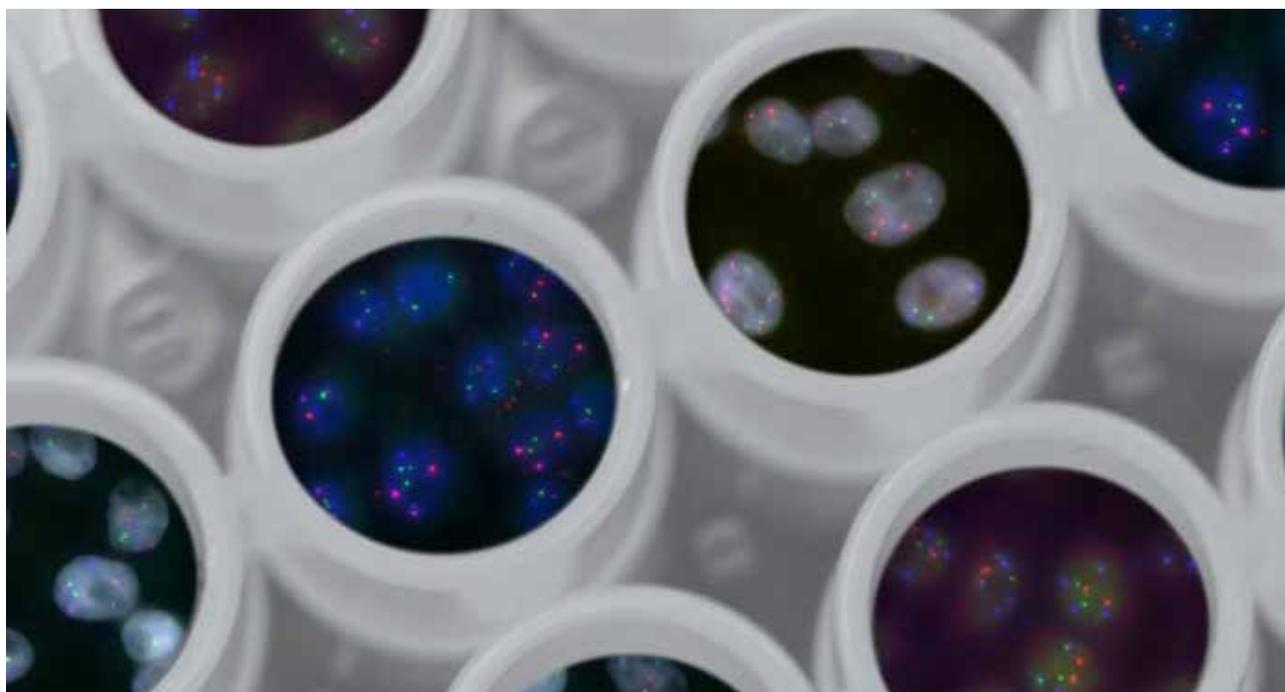
> **AI offers the potential to rapidly and cheaply predict protein structures, allowing scientists to examine the impact of genetic variations on macromolecules**

nately, it is difficult to predict some complex protein classes. AI offers the potential to rapidly and cheaply predict protein structures, allowing scientists to examine the impact of genetic variations on macromolecules. AI-based predictions are expected to improve our understanding of how genetic variation causes disease, enables drug development, and allows researchers to design specific proteins that break down plastics in nature. Consequently, protein-folding prediction is a significantly important domain

for the implementation of AI in biological sciences.

Recently, exponentially rapid implementation and advancement of AI in protein-folding prediction have yielded surprising results. In 2020, the company DeepMind made a major step forward with its algorithm AlphaFold at the 14th Community Wide Experiment on the Critical Assessment of Techniques for Protein Structure Prediction (CASP). AlphaFold predicted structures for a range of proteins with an accuracy over 90%, compara-

ble to conventional methods.[1] From this success, highly accurate protein structure prediction may soon promise benefits for public health, such as vaccine developments.

However, malicious actors might use protein-folding prediction algorithms for purposes unintended in their original development. Understanding how genetic variation affects protein structure may enable researchers to discover disease-causing mutations using one individual's genome sequence. While this ability

---

1   John Jumper, et al., High Accuracy Protein Structure Prediction Using Deep Learning In Fourteenth Critical Assessment of Techniques for Protein Structure Prediction (Abstract Book), (30 November - 4 December 2020)

> **However, malicious actors might use protein-folding prediction algorithms for purposes unintended in their original development**

might raise serious concerns for individuals who carry rare and/or severe genetic diseases, the threat would become even more significant if malicious actors could predict how genetic variations impact the severity of diseases and identify individuals susceptible to specific pathogens. These threats open the door to a dual-use technology dilemma and raise the question of how we can prevent malicious actors from weaponizing protein-folding prediction while still fostering scientific advancement.

As protein-folding prediction algorithms are still in the early stages of development, the ways they could be weaponized are also only beginning to be understood.[2,3,4] Although exploitation of this technology is perhaps still considered low risk to national security, malicious actors may have already been directed to consider how to exploit such advantages. While there is currently no evidence of nefarious individuals, organizations, or States having advanced their technologies and human resources to the extent of exploiting protein-folding AI systems, it is critical to raise awareness of potential threats. The evolving nature of criminal activities and rapid advancements in AI and biotechnology capabilities make it vital.[5]

One important aspect regarding the security of emerging technologies is the accessibility of source code. Although open science fosters scientific development, it should also be acknowledged that malicious actors can exploit

transparency for illicit purposes. Once a source code is released for an advanced AI, malicious actors could use or modify it to cause harm. Depending on the advancement of such technology, even the description of methodology or pseudo-code may be sufficient for malicious actors to recreate the technology partially or in full capacity. Thus, security challenges can arise when advances are made in AI, especially when the original developments are considered safe.

DeepMind did not immediately release its AlphaFold source code[6]. Nevertheless, in approximately seven months, academic researchers were able to use the general methodology to create an algorithm of their own that performed nearly as well[7]. The source code from this academic group was released along with a preprint at almost the same time that DeepMind published their peer-reviewed article and their own source code[8]. As more protein-folding prediction approaches

2   Sara B. Jordan, Samantha L. Fenn, and Benjamin B. Shannon, "Transparency as Threat at the Intersection of Artificial Intelligence and Cyberbiosecurity." Computer 53.10 (2020): 59-68.

3   Sterling Sawaya, Erin E. Kenneally, Demetrius Nelson, and Garrett J. Schumacher, "Artificial Intelligence and the Weaponization of Genetic Data" (April 24, 2020) https://ssrn.com/abstract=3635050 or http://dx.doi.org/10.2139/ssrn.3635050

4   John T. O'Brien and Cassidy Nelson, "Assessing the Risks Posed by the Convergence of Artificial Intelligence and Biotechnology," Health Security, 18.3 (2020): 219-227.

5   Sergio Bonin, "Challenges to Biosecurity from Advances in the Life Sciences," UN Chronicle https://www.un.org/en/chronicle/article/challenges-biosecurity-advances-life-sciences

6   https://deepmind.com/blog/article/alphafold-a-solution-to-a-50-year-old-grand-challenge-in-biology

7   Baek, Minkyung, Frank DiMaio, Ivan Anishchenko, Justas Dauparas, Sergey Ovchinnikov, Gyu Rie Lee, Jue Wang et al. "Accurate prediction of protein structures and interactions using a 3-track network." bioRxiv (2021) https://www.biorxiv.org/content/10.1101/2021.06.14.448402v1

8   Jumper, John, Richard Evans, Alexander Pritzel, Tim Green, Michael Figurnov, Olaf Ronneberger, Kathryn Tunyasuvunakool et al. "Highly accurate protein structure prediction with AlphaFold." Nature (2021): 1-11.

become available to the public, higher risks appear for malicious actors to exploit this advancement to design novel bioweapons. However, the solution to this threat should not be classifying these algorithms as a weapon and keeping their methodologies secret. On the contrary, considering the unprecedented opportunities this advancement promises, scientific engagement should be actively promoted while mitigating their risks.

One solution to prevent undesired dual-use scenarios of protein-folding prediction algorithms could be to design access schemes to their data, techniques, and outputs. Further publication and dialogue surrounding dual-use possibilities should be encouraged. These approaches would be complementary to a responsible innovation approach. Moreover, a substantial discussion about the ethics and dual-use potential of protein folding prediction should be initiated.

The dual-use threat of protein-folding prediction also highlights the importance of the security of medical facilities, research institutions, and biobanks. Any weaponization attempt of this technol-ogy cannot be made without training the subjected AI systems with genetic information extracted from samples given by the targeted individuals or populations. Unfortunately, during the COVID-19 pandemic, the number of cyber-attacks directed at hospitals, vaccine developers, and others have increased. Consequently, sensitive and valuable genetic information might be seized by malicious actors, although no major incident has been reported to date. While there is concern that exploitation of population sequence analysis could lead to the creation of targeted bio-weapons[9], dual-use of advancement of protein-folding predictions could have complementary effects on these threats or might even expedite such malicious efforts in the future. Institutions with databases of genetic information should therefore enhance their security against any threat. Moreover, we must ensure the utmost com-
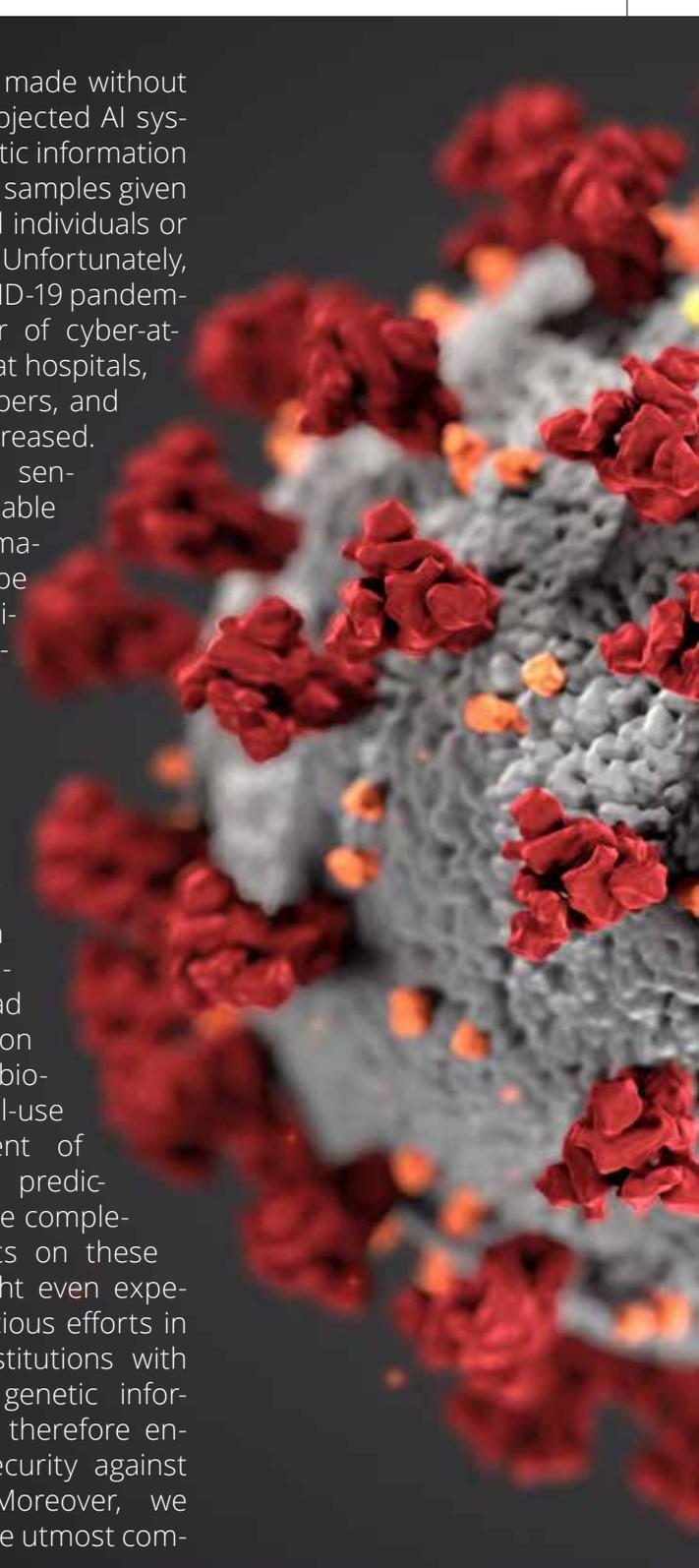
9   K.L. Warmbrod, J. Revill, and N. Connell, "Advances in Science and Technology in the Life Sciences: Implications for Biosecurity and Arms Control,"
      2020, Geneva, Switzerland: UNIDIR, https://unidir.org/publication/advances-science-and-technology-life-sciences

pliance with up-to-date data protection and research ethics principles.

Ultimately, DeepMind has made a ground-breaking advancement in a protein-folding prediction that offers tremendous promise for the good of humankind. Nevertheless, potential dual-use applications of such powerful algorithms could have undesirable effects. Considering the rapidly evolving nature of crime and the ongoing global effects of the COVID-19 pandemic, the manifestation of such threats might occur sooner than later. Thus, efforts to understand and prevent such scenarios in their earliest stages are crucial.

THE AUTHOR

Sterling Sawaya is the Founder & CEO, GeneInfoSec

Taner Kuru is an Intern at the United Nations Interregional Crime & Justice Research Institute (UNICRI)

Thomas A. Campbell, Ph.D., is the Founder & CEO, FutureGrasp

Publications

Download UNICRI publications

HEIs are in a unique position in society as they are considered neutral and influential players

INFOCUS

by Noel Klima, Juliana Martins Vasconcelos Senra and Jasmine De Backer

HIGHER EDUCATION INSTITUTIONS (HEIs) AND SDG 16: INTER- AND TRANSDISCIPLINARY COOPERATION TOWARDS IMPACT

Introduction

In 2015 all Member States of the United Nations (UN) adopted the Sustainable Development Goals (SDGs) – a voluntary set of objectives – also known as "Global Goals" or "2030 Agenda". Therefore, it is not surprising that many Higher Education Institutions (HEIs) worldwide choose to do so as well. HEIs comprise traditional universities, colleges, and other education institutions delivering high education, including applied sciences or polytechnique universities. They are all knowledge institutions that serve society through independent research, education, and societal service provision, making HEIs valuable partners in the collaborations aiming to promote the SDGs.

The Global Goals offer HEIs the opportunity to restructure their strategy and integrate sustainable development in their systems in a holistic way to respond to the current societal challenges.[1, 2] HEIs are in a unique position in society as they are considered neutral and influential players,[3,4]

> **HEIs are in a privileged position to reinforce the most effective skills in promoting justice and consensus, such as conflict resolution tools** which allows them to foster dialogue.

Their position stimulates and encourages interdisciplinary collaborations by bringing together expertise from various fields such as social sciences and humanities (SSH); science, technology, engineering and mathematics (STEM); medical sciences, and other related domains.[5] Likewise, partnerships with non-academic partners from industry, policymakers, and civil society actors (transdisciplinary collaborations) are gaining more relevance to approach the "wicked problems" of current times.[6] As critical and independent partners, HEIs can stimulate and catalyze change through inter- and transdisciplinary collaborations with other societal partners.

Goal 16 of the Sustainable Development Goals is dedicated to "promoting peaceful and inclusive societies for sustainable development, the provision of access to justice for all, and building effective, accountable institutions at all levels." On a holistic level, Goal 16 reflects the close interconnection uniting inequality, peace, and environmental questions to global development principles.

While education directly relates to SDG 4, it is transversal to all 17 goals. The relation between SDGs 4 and 16 is, as highlighted by 'UNESCO's 2019 Global Education Monitoring Report',[7] one of interdependence – education is not possible without the safety of peaceful and just societies, while education is vital in promoting these values.

The role of HEIs in the achievement of SDG 16

Following Sustainable Development Solutions Network's typology, there are four main fields in which HEIs can promote all SDGs: education, research, governance and operations, and external leadership.[9] Contributions to SDG 16 in these four fields can be found in the literature. We will clarify the role of HEIs in promoting peace, justice, and inclusivity by mapping these possibilities.

Regarding **education**, while it is a sustainability goal on its own, it enjoys a strong connection with SDG 16. Education for sustainable development that is inclusive and mobilizes youth for societal action is crucial for creating a sustainable future.[10] HEIs can increase knowledge on topics such as legal rights and environmental law. They can develop students' competencies to think through complexity and enhance their learning through dialogue and communication. They can inspire them to engage in deep reflection, develop a worldview, and value sensitivity.[11] HEIs are in a privileged position to reinforce the most effective skills in promoting justice and consensus, such as conflict resolution tools. They can foster values of gender awareness-raising, of non-discrimination, and advocate for participatory democracy.[12] In terms of integrating these subjects into the curriculum, there are two ways. A horizontal integration implies integrating sustainable development into the different courses and topics. The vertical integration involves creating specific courses focusing on the SDGs. The first option is seen as more effective as it tackles the complexity of sustainability questions.[13] HEIs' role in education can also go beyond the students enrolled. These institutions can provide tailored training on the SDGs to local stakeholders, such as NGOs, the private sector, and governmental institutions, and become partners in trans, it is transdisciplinary co-creation trajectories.[14]

Through **research**, HEI can contribute to evidence-based policymaking, for instance, by evaluating SDG indicators in an independent manner, such as an Egyptian case study indicates.[15] This contribution ensures that official and governmental data on SDGs implementation is scrutinized, meaning that HEIs and civil society actors can ensure that the evaluation of SDGs implementation is transparent and objective. The case study shows that this is particularly important for SDG 16, as state institutions express finding the reporting process on the matter extremely challenging. According to the "Asso-ciation for the Advancement of Sustainability in Higher Education's 2019 Technical Manual," it is important to ensure that research is open and accessible. This will strengthen the transparency and accountability of institutions and allow non-academics to access quality peer-reviewed research as reliable sources. Furthermore, research carried out in HEIs can contribute to the achievement of SDG 16 through applied or problem-solving research, through critical scholarship, and through the research process itself.[17]

In terms of **governance**, according to a study from Qatar's Center for Conflict and Humanitarian studies,[18,] HEIs can contribute towards achieving SDG 16 in conflict-affected contexts. HEIs can exert agency in political conflict resolution by, for example, ensuring academic freedom in the face of conflict so that political action can be assessed. They can also serve as mediators between local demands and the global logic of the SDGs as a peacebuilding model. An excellent example of how to put it into practice is in Sierra Leone's Makeni University. Its civic education program aims

Goal 16 reflects the close interconnection uniting inequality, peace, and environmental questions to global development principles

at consolidating the democratic system through voter education and the monitoring of elections, for example,[19] actively strengthening institutions' transparency and reliability. Additionally, HEIs' can support Goal 16 in conflict-affected regions by addressing the social, political and economic inequalities, and engaging constructively in identity politics.[20] They could also contribute by improving educational opportunities and attainment levels, which, as a result, could decrease the level of conflict.[21]

In another sense, HEIs can and should lead by example in relation to sustainable forms of governance – incorporating the spirit of SDG 16 in their regulations in issues of employment, finance, support services, and others is a way to promote sustainable forms of institutional governance.[22] Involving staff, students, and key stakeholders in HEIs' decisions or ensuring multicultural acceptance on campus, are practical ways for HEIs to pave the way.[23] Education should strive to be free from discrimination, violence and harassment, fostering skills through which the students can also fight inequality in their communities, according to The Commonwealth's 2017 Curriculum Framework for the Sustainable Development Goals.[24] This approach includes providing a gender-sensitive, rights-based, community-oriented, and inclusive education, mainly aimed towards vulnerable and marginalized groups while committing to end all forms of inequality.

> ❞
> **Education should strive to be free from discrimination, violence and harassment**

When it comes to **external leadership**, many have pointed out that HEIs provide education to the future 'sustainable development leaders'.[25] Young leaders with a sustainable mindset entering government institutions and the private sector, capable of stimulating the existing links between local and global societies.[26] With this in mind, it is crucial that HEIs strengthen public engagement and participation when addressing the SDGs, as exposing these future leaders to the UN's Agenda 2030 will hopefully influence their future institutional behavior. This can be achieved, for example, by providing educational opportunities such as lectures and workshops in which leading experts discuss topics of sustainability, but also by being vocal about HEIs'

interventions in policymaking and advocating for sustainable development.[27] The SDGs provide the opportunity to enhance this leadership role given that most HEIs already have the research and education expertise needed to build capacity and support policymaking,

HEIs and the community

The previous four categories focused mostly on how HEIs can singularly impact the promotion of SDG 16. Still, other sources point out the need to understand HEIs' role as one stakeholder amongst many. Establishing meaningful partnerships to achieve the SDGs can help to build "empirical and analytical consensus on problems and solutions, encourage cross-sectoral and interdisciplinary collaboration for innovation and provide cost-effective data and science-based evidence for policymakers and governments to address multiple goals and interlinkages across all SDGs."[28] In their 2019 study, Franco and Tracey highlight how HEIs, stakeholders, and communities can join forces in solving common problems through various bottom-up approaches under the umbrella term "community capacity-building initiatives."[29] Providing concrete examples, the authors suggest that practical skills enhancement (such as decision-making, ne-

gotiation, and communication skills, in both individual and collective senses), conceptual skills development (on topics such as peace, reconciliation, trust, and emotional intelligence), and community development (leadership, inclusion of indigenous knowledge and the search for local solutions) are areas in which HEIs can cooperate with other agents in the community.[30] The authors stress the importance of these initiatives being community-led as a whole, according to local needs, and respecting local knowledge. Thereby, they encourage initiatives to be taken beyond the HEIs.

Some authors have stressed how social sustainability issues are sometimes overlooked in sustainability initiatives compared to environmental sustainability issues. They highlight the need to understand the interconnectedness of

these topics. Participants of a 2018 qualitative study on how Higher Education for sustainable development can be integrated into policy, curriculum and practice, all agreed that focusing on 'diverse and vulnerable community groups such as indigenous communities and refugees'[31] could be a solution

HEIs, stakeholders, and communities can join forces in solving common problems through various bottom-up approaches

❝

to this, while also committing to the achievement of SDG 16.

An example of how HEIs can engage the community, particularly its most vulnerable members, can be found in De Montfort University's Global Hub for SDG 16.[32] Being the UN-certified hub for SDG 16 in HEI, this UK University develops a series of projects and multidisciplinary research on current peace and justice issues. One of these projects was the Local Refugee Support Programme, offering mentoring to young refugees to pursue further educations, skill development sessions in partnership with local charities (such as IT and language classes), and other activities that engaged community stakeholders.[33]

De Montfort University's Global Hub for SDG 16 also created specialized research groups, such as the Crimi-

nal Justice Research Group, that has recently developed projects on zero tolerance to slavery and human trafficking. In addition, they have created courses and programs, such as the International Human Rights LLM, focusing primarily on SDG 16 and promoting active learning through partnerships with civil society organizations, encouraging students to take action in refugee aid, for example. They are engaged with all four categories that the Sustainable Development Solutions Network (SDSN) identified as relevant for promoting the SDGs and engaging local stakeholders frequently, providing many examples of good practices.

Goal 16 evaluation

Another role HEIs can fulfill in the UN's Agenda for Sustainable Development is to thoroughly evaluate the SDGs implementation level in their activities. By doing so, HEIs can create resources that determine what areas need more attention and identify opportunities for future undertakings. At the same time, it can promote existing activities, stimulating students' informed involvement in these.[34]

The magazine "Times Higher Education" (THE) publishes an annual impact ranking on each SDG that exemplifies this evaluation methodology. It bases on four main criteria in the case of SDG 16: quantity and quality of research on peace and justice topics; university governance measures, such as student union's role, academic freedom protections, and engagement of local stakeholders; working with governments as experts or through policy-focused re-search; and the proportion of graduates in law and civil enforcement, as educating these practitioners will impact the future of institutions.[35]

Toronto University's Expanded Student Engagement Project[36] developed their evaluation and promotion project by creating three inventories that students could consult on sustainability-related opportunities beyond formal education. One of the inventories focused on community-engaged learning opportunities, another on co-curricular and extracurricular activities, and the third on sustainability presence in the university's courses. On this last matter, the university ascertained that 20% of the courses in the inventory included education on SDG 16, making it the second most present SDG after SDG 13 (Climate Action).[37]

> **They concluded that over 1200 courses provided education on one or several SDGs and that SDG 16 was one of the most covered**

Edinburgh University's Department of Social Responsibility and Sustainability established a curriculum review project to analyze the inclusion of the SDGs in their curriculum. The project consisted of an electronic appraisal of the Business School courses on Degree Regulations and Programmes of Study (DRPS) and a faculty survey that included staff and students. The project found that, respectively, only 7 and 10 percent of the search term hits related to SDG 16 in the undergraduate and postgraduate curriculum. In addition, staff experienced a lack of guidance on successfully integrating the sustainable development goals in their curriculum.[38]

Chang and Lien's study of NUK (the National University of Kaohsiung, in Taiwan)[39] similarly mapped the extent of SDG's embeddedness in the university's curriculum. They concluded that over 1200 courses provided education on one or several SDGs and that SDG 16 was one of the most covered.[40] When assessed in terms of different faculties, the law faculty revealed the most prevalence of SDG 16 inclusion in the curriculum. As the authors highlight, although there is an ordinary association between an SDG's thematic aim and the course's subject, it is evident that interdisciplinary approaches to SDGs are still lacking.

This one-sided thematic focus is stressed in other sources, in particular when it comes to the need for developing interdisciplinary connections, such as those between STEM and the social sciences and humanities (SSH), fostering a holistic understanding of

> **SDG 16 is thus seen as foundational to the conditions that can enable other Goals and a sustainable future to be attained**

165

sustainability. Engineering faculties, in particular, are found to often disregard the social aspects of sustainability, with a 2018 study finding SDG 16 to be of second-lowest importance for teachers and the least integrated into research.[41] The authors stress the importance of connectors between different research centers, transcending the boundaries of disciplines and the universities themselves, and engaging non-scientific stakeholders in research processes.[42]

❝

Need for joint efforts of HEIs, businesses, governments, and non-governmental organizations to launch community capacity-building initiatives towards achieving the SDGs Agenda

The evaluation of SDG 16 by students has, in the past, shown its centrality for HEI and the achievement of other SDGs. Mugisha's 2017 study, for example, focused on students' perceptions of what SDGs were most important for the future of their coun-

try, South Sudan.[43] They considered SDG 16 the most important since, as one student puts it, 'peace is a priority because it would allow other goals to be achieved'.[44] SDG 16 is thus seen as foundational to the conditions that can enable other Goals and a sustainable future to be attained.

Discussion and conclusions

HEIs have the capacity to generate, translate and disseminate knowledge relevant to achieving the SDGs and contribute to a just, peaceful, and inclusive society. By implementing active policies for developing SDGs through their education, research, governance, and external leadership activities, promoting awareness among other actors, and acquiring the skills and mindsets needed, HEIs play a key role in the 2030 Agenda.[45]

The rationale of Goal 16 is closely linked with criminology and criminal justice, as a fair and effective criminal justice system, the prevention of violence, and respect for human rights, are all essential elements for a peaceful and inclusive society.[46] However, interdisciplinary synergies are needed on the one hand, such as those between STEM and the social sciences and humanities (SSH). And on the other hand, transdisciplinary cooperation and partnerships with non-academic partners such as policy makers, civil society

actors and industry. Inter- and transdisciplinary approaches to the SDGs are fundamental in promoting the capacity to understand and act on 'wicked' problems and are essential to align education outcomes with the SDGs.

Furthermore, this contribution also highlights the need for joint efforts of HEIs, businesses, governments, and non-governmental organizations to launch community capacity-building initiatives towards achieving the SDGs Agenda without losing sight of the local needs and knowledge.

The growing awareness among Universities to play an active role, next to the traditional missions of education and research, and to engage in societal challenges (and market demands) to contribute to society (Third Mission of Universities) has been implemented differently depending on the socio-economic contexts of the Universities. For instance, at Ghent University a range of interconnected activities have been implemented to strengthen this Third Mission, such as the installation of 10 interdisciplinary research consortia with focus on societal impact (IDC).[47] Among others, the interdisciplinary consortium "IDC Crime, Criminology and Criminal Policy" has taken steps to include and engage key actors in a longterm and structural way. A noteworthy example is the CaST – Com-

munities and Students Together - project which focuses on how universities can work more effectively and inclusively within their city's communities by providing students with opportunities to work on local societal challenges.[48,49]

In addition to devising and implementing the inter- and transdisciplinary projects and initiatives, it is necessary to thoroughly evaluate the level of SDGs implementation in HEIs own activities and initiatives to formulate recommendations for further actions to support the 2030 Agenda. It

is also essential that HEIs map the inclusion of SDGs and disseminate the results to staff and students to enhance their working knowledge of SDGs and the underlying principles and use that knowledge in their future careers and personal lives.

THE AUTHORS

Noel Klima is IDC Coordinator and Head of Knowledge Transfer, Engagement and Societal Impact at the *IDC Crime, Criminology & Criminal Policy* at Ghent University in Belgium. He is leads a range of capacity building initiatives to foster knowledge transfer and societal value creation of crime an security research. He is Steering Group Member of the Business Development Center *i4S - Smart Solutions for Secure Societies* and Board Member of the youth welfare and resilience training organization *ARKTOS npo*. He is co-editor of the book Engaged learning in Europe (Maklu) and is lecturer in several engaged learning courses. Noel Klima holds a PhD Criminology and has broad experience working at the interface of research, practice and policy working in different organisations on national and international level.

Juliana Martins Vasconcelos Senra is Erasmus+ trainee at Ghent University's *IDC consortium 'Crime, Criminology & Criminal Policy'* based at the *Institute for International Research on Criminal Policy (IRCP)* at Ghent University in Belgium. She holds a Master of Sociology of Law at Lund University (Sweden) and a Bachelor in Law from Nova School of Law, in Lisbon. She has worked as a researcher in the area of gender equality and law at CEDIS, a research center on Law and Society based in Lisbon.

Jasmine De Backer is research assistant at the Ghent University's *IDC consortium Crime, Criminology & Criminal Policy* based at the *Institute for International Research on Criminal Policy (IRCP)*, Faculty of Law & Criminology at Ghent University in Belgium. She holds a Master in Criminology and is enrolled for the Master in Public Management at Ghent University.

167

REFERENCES

1 Leal Filho, W., Azeiteiro, U., Alves, F., Pace, P., Mifsud, M., Brandli, L., ... & Disterheft, A. (2018). Reinvigorating the sustainable development research agenda: the role of the sustainable development goals (SDG). *International Journal of Sustainable Development & World Ecology*, 25(2), 131-142.

2 Global University Network for Innovation (GUNi). (2019). Implementing the 2030 Agenda at Higher Education Institutions: Challenges and Responses.

3 El-Jardali, F., Ataya, N., & Fadlallah, R. (2018). Changing roles of universities in the era of SDGs: rising up to the global challenge through institutionalizing partnerships with governments and communities. *Health research policy and systems*, 16(1), 1-5.

4 Kestin, T., van den Belt, M., Denby, L., Ross, K. E., Thwaites, J., & Hawkes, M. (2017). *Getting started with the SDGs in universities: A guide for universities, higher education institutions, and the academic sector*. Sustainable Development Solutions Network.

5 Vilalta, J. M., Betts, A., & Gómez, V. (2018). Higher Education's role in the 2030 Agenda: The why and how of GUNi's commitment to the SDGs. In *Sustainable Development Goals: Actors and Implementation. A Report from the International Conference* (pp. 2018-06). GUNi: Barcelona, Spain.

6 Sáenz, O. (2019). *Implementation of the Sustainable Development Goals (SDGs) in higher education institutions: Recommendations based on the experience of a Latin American University. Implementing the 2030 Agenda at Higher Education Institutions: Challenges and Responses*

7 UNESCO (2019). *Global Education Monitoring Report. Migration, displacement, and education: Building Bridges, not Walls.* Paris, UNESCO. https://en.unesco.org/gem-report/report/2019/migration

8 Kestin, T., van den Belt, M., Denby, L., Ross, K. E., Thwaites, J., & Hawkes, M. (2017). *Getting started with the SDGs in universities: A guide for universities, higher education institutions, and the academic sector*. Sustainable Development Solutions Network.

http://ap-unsdsn.org/wp-content/uploads/University-SDG-Guide_web.pdf

9 Milton, S. (2021). Higher education and sustainable development goal 16 in fragile and conflict-affected contexts. *Higher Education*, 81(1), 89-108.

10 Kestin, T., van den Belt, M., Denby, L., Ross, K. E., Thwaites, J., & Hawkes, M. (2017). *Getting started with the SDGs in universities: A guide for universities, higher education institutions, and the academic sector*. Sustainable Development Solutions Network. http://ap-unsdsn.org/wp-content/uploads/University-SDG-Guide_web.pdf

11 Useh, U. (2021). Sustainable Development Goals as a Framework for Postgraduate Future Research Following COVID-19 Pandemic: A New Norm for Developing Countries. *Higher Education for the Future*, 8(1), 123-132.

12 Osman, A., Ladhani, S., Findlater, E., & McKay, V. (2017). Curriculum framework for the sustainable development goals. *The Commonwealth Secretariat*: UK. https://www.thecommonwealth-educationhub.net/wp-content/uploads/2017/01/Curriculum_Framework_for_SDGs_July_2017.pdf

13 Orlovic Lovren, V., Maruna, M., & Stanarevic, S. (2020). Reflections on the learning objectives for sustainable development in the higher education curricula– three cases from the University of Belgrade. *International Journal of Sustainability in Higher Education*, 21(2), pp. 316

14 Mugisha, F. (2017). Negotiating Sustained Action for Sustainable Development - Application to Students in South Sudan. *Global policy*, 8(4), pp. 586

15 El Baradei, L. (2019). Politics of Evidence-Based Policy Making: Reporting on SDG 16 in Egypt. *International Journal of Public Administration*, 43(5), pp. 430

16 AASHE (2019). STARS Technical Manual 2.2. https://stars.aashe.org/wp-content/uploads/2019/07/STARS-2.2-Technical-Manual.pdf

17 Milton, S. (2017). *Higher education and post-conflict recovery*. Springer.

18 Milton, S. (2021). Higher education and sustainable development goal 16 in fragile and conflict-affected contexts. *Higher Education*, 81(1), 89-108.

19 United Nations Academic Impact (2018, Augustus 14). *#SDGsinAcademia: Goal 16*. https://www.un.org/en/academic-impact/sdgsinacademia-goal-16., Last accessed 13/10/2020

20 Pherali, T., & Lewis, A. (2019). Developing global partnerships in higher education for peacebuilding: a strategy for pathways to impact. *Higher Education*, 78(4), 729-744.

21 Calderon, A. (2021, April 22). How can universities ensure progress towards the UN SDGs? *University World News*.

22 Kestin, T., van den Belt, M., Denby, L., Ross, K. E., Thwaites, J., & Hawkes, M. (2017). *Getting started with the SDGs in universities: A guide for universities, higher education institutions, and the academic sector*. Sustainable Development Solutions Network pp. 1, pp. 23, http://ap-unsdsn.org/wp-content/uploads/University-SDG-Guide_web.pdf

23 Kestin, T., van den Belt, M., Denby, L., Ross, K. E., Thwaites, J., & Hawkes, M. (2017). *Getting started with the SDGs in universities: A guide for universities, higher education institutions, and the academic sector*. Sustainable Development Solutions Network. pp. 26

24 Osman, A., Ladhani, S., Findlater, E., & McKay, V. (2017). Curriculum framework for the sustainable development goals. *The Commonwealth Secretariat*: UK. pp. 78, pp. 81. https://www.thecommonwealth-educationhub.net/wp-content/uploads/2017/01/Curriculum_Framework_for_SDGs_July_2017.pdf

25 Kestin, T., van den Belt, M., Denby, L., Ross, K. E., Thwaites, J., & Hawkes, M. (2017). *Getting started with the SDGs in universities: A guide for universities, higher education institutions, and the academic sector*. Sustainable Development Solutions Network. http://ap-unsdsn.org/wp-content/uploads/University-SDG-Guide_web.pdf

26 Chang, Y.-C., & Lien, H.-L. (2020). Mapping Course Sustainability by Embedding the SDGs Inventory into the University Curriculum: A Case Study from the National University of Kaohsiung in Taiwan. *Sustainability*, 12(10), 4274, pp. 1

27 Kestin, T., van den Belt, M., Denby, L., Ross, K. E., Thwaites, J., & Hawkes, M. (2017). *Getting started with the SDGs in universities: A guide for universities, higher education institutions, and the academic sector*. Sustainable Development Solutions Network. http://ap-unsdsn.org/wp-content/uploads/University-SDG-Guide_web.pdf

28 Nelles, W. (2017, 28 March). *University Partnerships and Innovations Contributing to the ASEAN Work Plan on Education*, 2016-2020 PowerPoint-slides .

29 Franco, I. B., & Tracey, J. (2019). Community capacity-building for sustainable development. *International Journal of Sustainability in Higher Education*, 20(4), pp. 695

30 Franco, I. B., & Tracey, J. (2019). Community capacity-building for sustainable development. *International Journal of Sustainability in Higher Education*, 20(4), pp. 702

31 Franco, I., Saito, O., Vaughter, P., Whereat, J., Kanie, N., & Takemoto, K. (2018). Higher education for sustainable development: actioning the global goals in policy, curriculum, and practice. *Sustainability Science*, 14(6), pp. 1634

32 De Montfort University. (n.d.) *Sustainable Development Goals*. https://www.dmu.ac.uk/community/sdg/index.aspx

33 United Nations Academic Impact (2018, Augustus 14). *#SDGsinAcademia: Goal 16.* https://www.un.org/en/academic-impact/sdgsinacademia-goal-16

34 Kestin, T., van den Belt, M., Denby, L., Ross, K. E., Thwaites, J., & Hawkes, M. (2017). *Getting started with the SDGs in universities: A guide for universities, higher education institutions, and the academic sector*. Sustainable Development Solutions Network.

35 The World University Rankings. (2020, April 17). *THE Impact Rankings 2020 by SDG: peace, justice, and strong institutions (SDG 16) methodology.* https://www.timeshighereducation.com/impact-rankings-2020-sdg-peace-justice-and-strong-institutions-sdg-16-methodology

36 Brugmann, R., Côté, N., Postma, N., Shaw, E., Pal, D., & Robinson, J. (2019). Expanding Student Engagement in Sustainability: Using SDG- and CEL-Focused Inventories to Transform curriculum at the University of Toronto. *Sustainability*, 11(2), 530.

37 Brugmann, R., Côté, N., Postma, N., Shaw, E., Pal, D., & Robinson, J. (2019). Expanding Student Engagement in Sustainability: Using SDG- and CEL-Focused Inventories to Transform curriculum at the University of Toronto. *Sustainability*, 11(2), 530, pp. 10

38 University of Edinburgh. (2020). *Mapping the Sustainable Development Goals (SDGs) in the University Curriculum.*

39 Chang, Y.-C., & Lien, H.-L. (2020). Mapping Course Sustainability by Embedding the SDGs Inventory into the University Curriculum: A Case Study from the National University of Kaohsiung in Taiwan. *Sustainability*, 12(10), 4274

40 Chang, Y.-C., & Lien, H.-L. (2020). Mapping Course Sustainability by Embedding the SDGs Inventory into the University Curriculum: A Case Study from the National University of Kaohsiung in Taiwan. *Sustainability*, 12(10), 4274

41 Lazzarini, B., Pérez-Foguet, A., & Boni, A. (2018). Key characteristics of academics promoting Sustainable Human Development within engineering studies. *Journal of Cleaner Production*, 188, pp. 245

42 Lazzarini, B., Pérez-Foguet, A., & Boni, A. (2018). Key characteristics of academics promoting Sustainable Human Development within engineering studies. *Journal of Cleaner Production*, 188, pp. 245

43 Mugisha, F. (2017). Negotiating Sustained Action for Sustainable Development - Application to Students in South Sudan. *Global Policy*, 8(4), 582–586.

44 Mugisha, F. (2017). Negotiating Sustained Action for Sustainable Development - Application to Students in South Sudan. *Global policy*, 8(4), pp. 585

45 Ferguson, T., & Roofe, C. G. (2020). SDG 4 in higher education: Challenges and opportunities. *International Journal of Sustainability in Higher Education*.

46 Penal Reform International and Thailand Institute of Justice (2017). *The Sustainable Development Goals and Criminal Justice. (Global Prison Trends, Special Focus 2017).*

47 Ghent University's IDC Consortia https://www.ugent.be/en/research/science-society/idc/overview.htm

48 Klima, N., & Marsh, C. (2020). The interdisciplinary CaST project as inspiration for criminology education? In *EUROCRIM 2020, 20th Annual Conference of the European Society of Criminology, Book of Abstracts* (pp. 6–7). Online.

49 Marsh, C., Anderson, L., & Klima, N. (Eds.). (2021). Engaged learning in Europe. Antwerp: Maklu.

WE ARE ALL VULNERABLE

by Dimitri Dimitracacos

The true
measure of
any society
can be
found in
how it treats
its most
vulnerable
members

Mahatma Gandhi

Solidarity 'Missing in Action'

Secretary-General UN Secretary-General António Guterres' addressing the General Assembly.

We face the greatest cascade of crises in our lifetimes. The COVID-19 pandemic has supersized glaring inequalities. The climate crisis is pummelling the planet. Upheaval from Afghanistan to Ethiopia to Yemen and beyond has thwarted peace.

A surge of mistrust and misinformation is polarizing people and paralysing societies. Human rights are under fire. Science is under assault. And economic lifelines for the most vulnerable are coming too little and too late — if they come at all.

Wherever there is a human being, there
is an opportunity for a kindness
Lucius Annaeus Seneca

When people live in a fair, caring society, where everyone has equal access to social goods, they don't have to spend their time worrying about how to cover their basic needs day to day – they can enjoy the art of living. And instead of feeling they are in constant competition with their neighbours, they can build bonds of social solidarity

Jason Hickel

And if anyone saved a life, it would be as if he saved the life of the whole people

The Qur'an 5:32

WE ARE ALL
VULNERABLE

Our work for peace must begin within the private world of each of us. To build for man a world without fear, we must be without fear. To build a world of justice, we must be just.
DAG HAMMARSKJOLD

I am just a human being trying to make it in a world that is rapidly losing its understanding of being human.
JOHN TRUDELL

When people live in a fair, caring society, where everyone has equal access to social goods, they don't have to spend their time worrying about how to cover their basic needs day to day – they can enjoy the art of living. And instead of feeling they are in constant competition with their neighbours, they can build bonds of social solidarity.
JASON HICKEL

In spite of everything, I still believe that people are really good at heart.
ANNE FRANK

Entre pauvres gens, faut bien qu'on s'aide … C'est les grands qui font la guerre.
GUY DE MAUPASSANT

DIMITRI DIMITRACACOS is a photographer of Greek origins. He developed an interest in photography in his childhood and soon started working for Condé Nast and several famous photographers. At the same time, he started developing some personal projects allowing him to define his style, in particular in black and white on film. Around 2000, he started a career as a free-lance photographer with assignments from many different magazines. His passion for photography has extended over the time to other fields like street-photography and portrait and these are exactly the fields he has chosen to examine in depth for some time now. In 2019 he was the author of UNICRI's campaign "I am no longer myself" on violence against women.

177