**DISEC**  
  
  
TOPIC A : Preventing the Proliferation and Use of Chemical and  
Biological Weapons in Armed Conflict  
  
DEFINING THE PROBLEM  
  
The researchers pored over reports of chemical attacks going back to  
2012, reviewing the available information on each to verify the  
details. They collected evidence from "Syrian and international  
non-governmental organizations, monitoring groups, private firms,  
local administrative bodies, relevant international bodies, local and  
international media, and the open source."  
  
The report's authors attributed 2 percent of the chemical weapons  
attacks in Syria to the Islamic State.  
  
Syrian President Bashar Assad's regime carried out 98 percent of them,  
according to the authors, dropping chlorine gas, sarin and sulfur  
mustard gas on Syrian civilians.  
  
"It is clear that the Syrian military has consistently prioritized  
striking population centers over rebel positions on the frontlines,  
even in the face of defeat on the ground," they write.  
  
  
Most of these chemical attacks, the report concludes, came after  
August 2013, when a sarin attack outside Damascus left more than 1,400  
people dead. President Obama said then that the U.S. would take  
military action against Syria, with congressional approval. Instead,  
the U.S. entered talks with Russia and formed a resolution calling for  
Syria to get rid of its chemical weapons.  
  
A year later, the U.S. announced that Syria's chemical weapons had  
been destroyed. But chlorine wasn't part of the deal. As NPR's David  
Welna has reported, "Unlike other substances that fall under the  
treaty, such as sarin and mustard gas, chlorine is also produced and  
used in Syria for peaceful purposes, from cleaning products to water  
purification."  
  
Still, the State Department said in 2014 that chlorine attacks would  
violate the Chemical Weapons Convention, which bans the use of  
chemical weapons in war and which Syria has signed.  
  
Researchers at the Global Public Policy Institute found that the vast  
majority of the attacks since 2012 — 91.5 percent — have been chlorine  
bombs.  
  
  
  
Their report comes just a month after the U.S. began withdrawing from  
Syria. President Trump announced via tweet in December, "After  
historic victories against ISIS, it's time to bring our great young  
people home!"  
  
  
Since 2013, thousands of Syrians have been injured and hundreds killed  
by chemical warfare.  
  
The first chemical attack on record in Syria was in March 2013 near  
Aleppo. Since then, 17 locations have been attacked with chemical  
weapons.  
  
One year ago, sarin gas (or a sarin-like substance) was used to attack  
the town of Khan Sheikhoun. On the anniversary of that attack, Al  
Jazeera looks at the various chemical weapons used to attack  
rebel-held areas since 2013:  
  
Sarin  
  
Sarin gas is odourless and tasteless and works immediately to inhibit  
natural processes that control neurotransmitters in the body. The  
nerves are overstimulated uncontrollably, and the afflicted person's  
nose starts running, eyes crying, and they vomit continuously as their  
bowel and bladder evacuate themselves. Depending on the level of  
exposure, sarin gas can cause death within 10 minutes.  
  
White phosphorus  
  
White phosphorus has been used in conflicts since World War I. It is  
highly efficient at creating smoke and is used to cover troop  
movements or positions in conflicts. Exposure to white phosphorus  
causes severe burns as the gas sticks to the skin and causes severe  
burns that can result in the absorption of phosphorus into the organs  
of the body. In addition, inhalation of phosphorus smoke or fumes, as  
well as the oral ingestion of as little as 15mg can affect the body's  
organs and bones, sometimes causing death.  
  
Chlorine gas  
  
Used as a chemical weapon in World War I, chlorine gas is dispersed  
when pressurised chlorine is delivered via any explosive device. An  
everyday chemical with many peace-time uses, chlorine is readily  
available and exists in a grey area as a chemical weapon. Exposure to  
chlorine gas causes respiratory distress, severe irritation to the  
respiratory tract and eyes, and, depending on the level of exposure,  
can cause lasting damage to both.  
  
Mustard gas  
  
Mustard gas, or sulfur mustard, is a yellowish brown gas that has an  
odour resembling mustard, garlic or horseradish. It is a blistering  
agent, causing severe blisters on the skin and in the lungs. The  
effects of mustard gas are not immediate, and victims can start  
showing symptoms up to 24 hours after exposure, with chemical burn  
blisters appearing all over the body and, in some cases, damage to eye  
tissue and lungs. Severe mustard gas burns (on more than 50 percent of  
the body) can be fatal, and mustard gas victims are said to be more  
likely to develop cancer later in life. It was used towards the end of  
World War I and during the Iraq-Iran war between 1979-1988.  
  
  
COUNTRIES WITH CRUCIAL ROLES (EXCEPT SYRIA)  
  
  
United States of America  
  
US National Security Adviser John Bolton has warned the Syrian  
government that it should not see the impending US military withdrawal  
from the country as an invitation to use chemical weapons. Chemical  
and biological weapon usage seems to be a serious threat against the  
U.S since there are thousands of U.S armed forces members in the  
Middle East, especially in Syria.  
  
  
Russia  
  
In early 2018, Washington's top diplomat has accused Moscow of  
breaching "its commitments" to destroy Syria's chemical weapons  
stockpiles, following reports of a new attack near Damascus. Syria has  
dismissed the reports as "lies."  
  
In turn, Russia's Deputy Foreign Minister Sergei Ryabkov dismissed the  
claims as a smear campaign.  
  
"The fact that they keep repeating these dirty and false accusations  
against us, only shows the level of the US diplomacy," Ryabkov told  
the Interfax news agency. The diplomat also said US was using the  
accusations to hamper Russia's peace efforts.  
  
The Damascus regime said the reports of the attack were "lies" and a  
part of "the systematic aggressive and hostile policy of the West  
towards Syria," according to Syria's foreign ministry.  
  
Syrian authorities have repeatedly denied using chemical weapons on  
their territory.  
  
  
Turkey  
  
Kurdish doctors in Syria accused Turkey of using chemical weapons in  
an offensive on Afrin, after several civilians were treated for  
symptoms of poison gas.  
  
Turkish Government has denied the allegations, saying its forces do  
not use "banned ammunition" or keep chemical weapons in their arsenal.  
  
  
POSSIBLE SOLUTIONS TO THE PROBLEM  
  
It is crucial that, in uncertain times, nations do not fall back on  
using chemical weapons. In the past few years, political positions and  
structures that served people well for decades have been questioned.  
Insecure countries might become more willing to apply chemical weapons  
to harm opponents and secure strategic advantages.  
  
A new mindset is needed. It is impossible to ban every chemical that  
could be used to make a weapon, because almost all of them have other  
applications. For example, chlorine is a common industrial reagent as  
well as a suffocating gas. More than 60 million tonnes are produced  
each year and used for purifying water and manufacturing plastics,  
solvents and pharmaceuticals. Organophosphates are the basis of  
insecticides and herbicides as well as precursors of nerve agents.  
Many deadly compounds are easy for any professional chemist to make,  
with access to the right materials.  
  
There are two solutions: monitor the production and distribution of  
certain key chemicals (such as organophosphates) that might be  
misused; and train chemists to be aware of potential security risks.  
  
Meanwhile, chemists in industry and academia must sign up to a code of  
conduct surrounding the production, sale and use of chemicals,  
especially those listed in the CWC. Each time a chemical weapon is  
used, the reputation of chemists and the chemicals industry is  
imperilled.  
  
To reiterate, we need to do two things to limit chemical weapons:  
control the ingredients and improve ethical standards in the chemical  
profession.  
  
Banning chemicals is impossible because almost all the relevant  
chemicals required for making chemical weapons have good uses as well  
as bad. For example, isopropyl alcohol (IPA) is widely used as a  
solvent; millions of tonnes are used each year in the production of a  
range of products, including household cleaners, pesticides and  
personal-care products. Yet react IPA with methylphosphonyl  
difluoride, and you produce the nerve agent sarin.  
  
Meanwhile, the chemistry community — in both academia and industry —  
needs to become more aware of the potential misuse of certain  
chemicals. For example, in the 1990s, a colleague of mine inspected  
the main Iraqi facility that produced chemical weapons in the 1980s —  
the Muthanna State Establishment, northwest of Baghdad. To his  
disbelief, he discovered 4,000 tonnes of weapons ready to be launched  
(mainly mustard gas and cyclosarin), as well as 20,000 tonnes of  
precursor chemicals for making them. Storerooms were filled with  
barrels of thionyl chloride — an industrial chemical listed under the  
CWC as having possible weapons uses. Many of these were bought from  
European companies. Presumably no red flags were raised among company  
staff when the sizes of the Iraqi orders went from kilograms to  
tonnes.

TOPIC B: Restricting and Preventing Cyber Warfare and its Impacts

GENERAL LOOK AT THE TOPIC

Cyber-security researchers have identified a total of at least 57 different ways in which cyber-attacks can have a negative impact on individuals, businesses and even nations, ranging from threats to life, causing depression, regulatory fines or disrupting daily activities.

The researchers, from Kent's School of Computing and the Department of Computer Science at the University of Oxford, set out to define and codify the different ways in which the various cyber-incidents being witnessed today can have negative outcomes.

They also considered how these outcomes, or harms, can spread as time passes. The hope is that this will help to improve the understanding of the multiple harms which cyber-attacks can have, for the public, government, and other academic disciplines.

Overall the researchers identified five key themes under which the impact -- referred to in the article as a cyber-harm -- from a cyber-attack can be classified:

Physical/Digital

* Economic
* Psychological
* Reputational
* Social/societal

Each category contains specific outcomes that underline the serious impact cyber-attacks can have. For example, under the Physical/Digital category there is the loss of life or damage to infrastructure, while the Economic category lists impacts such as a fall in stock price, regulatory fines or reduced profits as a possibility.

In the Psychological theme, impacts such as individuals being left depressed, embarrassed, shamed or confused are listed, while Reputational impacts can include a loss of key staff, damaged relationships with customers and intense media scrutiny.

Finally, on a Social/Societal level, there is a risk of disruption to daily life such as an impact on key services, a negative perception of technology or a drop in internal morale in organisations affected by a high-level incident.

The full list of cyber harms can be viewed online.

The researchers point to high-profile attacks against Sony, JP Morgan and online dating website Ashley Madison, as examples where a wide variety of negative outcomes were experienced, from reputational loss, causing shame and embarrassment for individuals or financial damage.

They say these incidents underline why a taxonomy of impacts and harms is so important for businesses. Many successful cyber-attacks have been traced to exploits of well-known vulnerabilities that had not been dealt with appropriately because of a lack of action by firms who did not appreciate the ways in which they could be affected by a cyber-attack.

By providing a detailed breakdown of the many different ways a cyber-attack can impact a business and third-parties, it gives board members and other senior staff a better understanding of both direct and indirect harms from cyber-attacks when considering the threats their organisation faces. This also equally applies to other organisations and even governments or those who manage critical national infrastructure.

Commenting on the article, Dr Jason R.C. Nurse from the School of Computing: 'It's been well understood that cyber-attacks can have numerous negative impacts. However, this is the first time there has been a detailed investigation into what these impacts are, how varied they can be, and how they can propagate over time. This base figure of 57 underlines how damaging cyber-incidents can be and we hope it can help to better understand how a business, individual or even nation is affected by a cyber-attack. This is going to be even more relevant as everything and everyone becomes connected and the Internet of Things is fully realised.'

POSSIBLE RESULTS OF CYBER ATTACKS

A successful cyber attack can cause major damage to the businesses. It can affect the bottom line, as well as the business' standing and consumer trust. The impact of a security breach can be broadly divided into three categories: financial, reputational and legal.

### Economic Cost of Cyber Attacks

Cyber attacks often result in substantial financial loss arising from:

* theft of corporate information
* theft of financial information (eg bank details or payment card details)
* theft of money
* disruption to trading (eg inability to carry out transactions online)
* loss of business or contract

Businesses that suffered a cyber breach will also generally incur costs associated with repairing affected systems, networks and devices.

### Reputational Damage

Trust is an essential element of customer relationship. Cyber attacks can damage a business' reputation and erode the trust that customers have for the company. This, in turn, could potentially lead to:

* loss of customers
* loss of sales
* reduction in profits

WHAT CAN BE DONE?

### How to Minimise the Impact of Cyber Attacks on Businesses

Security breaches can devastate even the most resilient of businesses. It is extremely important to manage the risks accordingly. After an attack happens, an effective [**cyber security incident response plan**](https://www.nibusinessinfo.co.uk/content/cyber-security-incident-response-plan) can help:

* reduce the impact of the attack
* report the incident to the relevant authority
* clean up the affected systems
* get your business up and running in the shortest time possible

Namely, the easiest way for cyber criminals to attack is through negligent or poorly trained individuals. What is more, many crewmembers still doubt the importance of cyber security on their ship. But this is not true.

### Cyber security needs proper trained staffing to understand the full value of technology investments and the IT procedures. In order to engage more people in the subject, Gard suggests creating an analogy between the cyber threats and the other dangers of the maritime adventure.

Today, any company can be vulnerable to cyber risks. These can include:

* **Social engineering**: Hackers attempt to gain critical information;
* **Electronic GPS spoofing**: The creation of problems in the GPS info;
* **Phising scams**: Attempts to gain personal information by scam e-mails.

These attacks are happening more and more, but the good news is that there are ways to prevent them.

**Do not let anyone uninvited into the system**

This will be achieved by:

* Securing the computers, by using antivirus and updating the systems;
* Update ship operation systems;
* Use only company-approved software.

**Personal awareness**

* Be very careful about the e-mails you are receiving;
* Search the facts, such as the name of the person/company that sent the e-mail.

**Infiltration by malware**

In order to prevent a cyber criminal by infiltrating through a malware:

* Never insert anything on the computer before making sure it is clean;
* Check the device that you want to insert offline for viruses;
* Do not let third parties enter data alone.

**Physical protection**

Just like a door, computers must be protected physically as well. This can be done by:

* Using ID card authentication;
* Using long passwords of at least 8 characters that contain upper and lower letters, numbers and symbols;
* Protect your passwords.

**Segregated networks**

* No personal items must be connected to sensitive networks;
* Secure the stations for file sharing;
* Be careful what you share online and put tape over the camera and laptop on your computer.

