National Science and Technology Forum

S.E.T. for socio-economic growth

Message from the NSTF Executive Director

Technology drives war drives technology?

It is a conundrum as old as the history of humankind. From the invention of stone carved axes to the swift subjection of indigenous peoples all over the world by European colonial powers. From duals fought with different types of swords, to the tanks in World Wars I and II. Despite all this experience, over tens of thousands of years, humankind has not been able to devise the means to prevent war. There are mechanisms like international treaties, peace accords, diplomacy, peacekeeping forces, etc. Yet somehow, if a government is determined to wage a war, it will. For some of us oriented towards science and technology, this poses a moral dilemma time and again. The creation of technologies is in the hands of scientists, or people with superb technical skills, engineers, and innovators. Yet, the use of many technologies is in the hands of politicians, businessmen, leaders and/or criminals. The ethical application of technology is never guaranteed. Albert Einstein produced the ground breaking science that made the nuclear bomb possible. He made it known to the US government, together with his fellow scientists, that he strongly disapproved of the bomb in no uncertain terms. Yet, not long afterwards, the bombs that were developed using his science were dropped on Hiroshima and Nagasaki, causing unprecedented destruction and tragedy.

The world has been living with the spectre of nuclear war ever since. There were attempts at voluntary disarmament of countries with the capability to produce nuclear weapons, and a treaty was signed for the non-proliferation of nuclear weapons. Many will remember the cold war years, with the Soviet Union and the USA in a standoff over nuclear weapons for a long period of time. South Africa did its part after the ANC came into power in 1994 by destroying its nuclear arsenal.

21st century war

Now, as the rest of the world can see tragedies in Ukraine in (close to) real time thanks to current communications technology, it is clear that various technologies (old and new) are being used to enable genocide and for the burnt-earth approach that Russia is committing, as well as to defend Ukraine and oppose the Russians. Ukraine is of course not the only place in the world where tragedies and human rights are occurring, nor is it the first time for Ukraine. However, the current war following on Russia's invasion in February gives rise to globally felt effects and fear. It holds the attention of the public in developed countries as no other recent war has done. The reasons include that a third world war is anticipated and the possibility of a global nuclear war is closer than ever. They fear the destruction of everything that gives people of the 'developed' world a good standard of living, including safety (from war), education and health services, the possibility of prosperity, and relative stability of economies and countries.

Looking into the future, will there ever be a time when all of humanity agrees that there should be no more war? The prospects do not look good, and history has shown us that this has never worked. Perhaps this is the domain of the social sciences and humanities rather than science and technology. As long as people hang on to the technological version of 'survival of the fittest', there is no hope of preventing the devastation and cruelty of war.

The use of electronic technologies must be the biggest difference between World War II and modern warfare. Drones, satellites and electronic communications are now weapons. Artificial Intelligence is playing its part. The countries who can wield these most effectively have the best chances of winning battles and wars, while minimising their own losses. For example, the deployment of sophisticated

weapons and methods, including drones, by the United States (US) to cause destruction and death in a number of countries. The same mentality applies here as in the case of the Hiroshima and Nagasaki attacks: the bomber sits high above the target, unable to see his victims before and while he wreaks devastation on them. There is hardly any risk to themselves. In the case of drone warfare, the bomber is remote and shielded from danger and identification. The politicians who ordered the bombings sit at home, out of harm's way, and relish the numbers of deaths, maiming and destruction of infrastructure.

In the case of the war in Ukraine, who has the deadliest firepower?

Although Russia is managing to murder, maim, destroy and commit human rights abuses, Ukraine is managing to put up a steady resistance with the help of weapons from other countries.

An interesting example of re-purposing technology for war is that drones available in shops and for order on the internet, meant as toys and state-of-the-art cameras, are apparently used by Ukrainians to see where the Russian attackers are, which enables them to take cover or shoot missiles at the Russians. Another example is: High-Power E-Bikes Are Helping Ukrainians Stop Russian Invaders (msn.com)

Is there is a kind of 'democratisation' of war in that ordinary civilians can fight back, without training?

Cyberwar

Another case in point is cyberwar. Sabotage is enabled by the hacking of vast electronic data systems. In contrast to the bombs and missiles, this cyberwar is raging silently, mostly out of sight of the ordinary citizens of countries, even those who are engaged in combat.

It is difficult to get a true picture of what cyberwars are raging, but from a web search it seems that the instances, variety and sources are vast. Cyberattacks are also extremely frequent. It is not always possible to identify the sources, or even the countries from which the cyberattacks originate.

In general, the reasons for launching cyberattacks include extortion and other ways of making money off the victim. The means of achieving this include downloading ransomware onto the victim's computer. Another motive for cyberattacks is obtaining information from the victim's computer. This is achieved with spyware. Perhaps the aim here is mainly to steal passwords and personal information to use for further hacking or for identity theft. But I am sure that this would also be used for obtaining strategic information belonging to a country. A further function of cyberattacks is to spread propaganda and misinformation. However, some cyberattacks seem to be aimed simply at destruction of data and software, without a financial motive. I think it would be fair to say that the aim of such a hack is sabotage.

Countries have long been nervous of cyberattacks of Russian origin, and individuals, governments and institutions have indeed been victims of these. However, cyberattacks go both ways and it is difficult for the public to know the extent of cyberwar on Russia. It is also unclear to what extent such hacks are made by individuals or on behalf of the governments of these countries. The governments monitoring cyberattacks would have a better idea, but it seems to me that there would nevertheless be a wide margin of uncertainty.

Of greatest concern must be cyberattacks that disable or destroy infrastructure. Just before and after the launch of the invasion of Ukraine by Russia, the governments of western countries were fearful of the data systems of their departments and agencies being hacked by Russia. For example, the heads of state of the US and United Kingdom expressed their concern and warned citizens to take cyber-safety measures. Members of the public cannot yet know whether the concern was or is justified, but it is said that the threat of damaging cyberwar by Russia did not materialise. Is this propaganda or reality? Where Russian attacks on government websites have taken place, they were swiftly restored.

Can the cyberwar be won? My impression is that Russia is unlikely to win the cyberwar, because of the sophistication of cyber-defence in the opposing countries. This is speculation on my part as perhaps there are no hack-proof electronic systems. We cannot know at this stage the exact extent of the hacking of Russian state infrastructure by the US and other Western governments. Speculatively, this could potentially bring the Russian government to its knees, together with other methods like the

disabling of international banking transactions, which is already being done. Electronic systems are so much a part of modern banking, that this could perhaps also count as electronic warfare, if not cyberwar.

Background

Wikipedia has a page on cyberwar against Ukraine, which gives a detailed description of what is publicly known on this topic: 2022 Ukraine cyberattacks - Wikipedia.

I include some extracts with comments here for those who may be interested in a more detailed background:

> *During the prelude to the 2022 Russian invasion of Ukraine and the 2022 Russian invasion of Ukraine, multiple cyberattacks against Ukraine were recorded, as well as some attacks on Russia. The first major cyberattack took place on 14 January 2022, and took down more than a dozen of Ukraine's government websites.[1] According to Ukrainian officials, around 70 government websites, including the Ministry of Foreign Affairs, the Cabinet of Ministers, and the Security and Defense Council, were attacked. Most of the sites were restored within hours of the attack.[2] On 15 February, another cyberattack took down multiple government and bank services.[3][4]*
>
> *On 24 February, Russia launched a full-scale invasion of Ukraine. Western intelligence officials believed that this would be accompanied by a major cyberattack against Ukrainian infrastructure, but this threat did not materialize.[5] Cyberattacks on Ukraine have continued during the invasion, but with limited success. Independent hacker groups, such as Anonymous, have launched cyberattacks on Russia in retaliation for the invasion.[5][6]*

Just before the military attack on Ukraine, Russia launched cyberattacks. In the end these seem not to have been destructive, but rather to spread fear among the Ukrainian government officials and the population. The attacks included the State Emergency Service.

Wikipedia says: “The software, designated DEV-0586 or WhisperGate, was designed to look like ransomware, but lacks a recovery feature, indicating an intent to simply destroy files instead of encrypting them for ransom.[10] “

> *The attacks on 14 January 2022 consisted of the hackers replacing the websites with text in Ukrainian, erroneous Polish, and Russian, which state "be afraid and wait for the worst" and allege that personal information has been leaked to the internet.[7] About 70 government websites were affected, including the Ministry of Foreign Affairs, the Cabinet of Ministers, and the Security and Defense Council.[8] The SBU has stated that no data was leaked. Soon after the message appeared, the sites were taken offline. The sites were mostly restored within a few hours.[1] Deputy secretary of the NSDC Serhiy Demedyuk, stated that the Ukrainian investigation of the attack suspects that a third-party company's administration rights were used to carry out the attack. The unnamed company's software had been used since 2016 to develop government sites, most of which were affected in the attack.[8] Demedyuk also blamed UNC1151, a hacker group allegedly linked to Belarusian intelligence, for the attack.[9]*
>
> *A separate destructive malware attack took place around the same time, first appearing on 13 January. First detected by the Microsoft Threat Intelligence Center (MSTIC), malware was installed on devices belonging to "multiple government, non-profit, and information technology organizations" in Ukraine.[10] Later, this was reported to include the State Emergency Service and the Motor Transport Insurance Bureau.[11] The software, designated DEV-0586 or WhisperGate, was designed to look like ransomware, but lacks a recovery feature, indicating an intent to simply destroy files instead of encrypting them for ransom.[10] The MSTIC reported that the malware was programmed to execute when the targeted device was powered down. The malware would overwrite the master boot record (MBR) with a generic ransom note. Next, the malware downloads a second .exe file, which would overwrite all files with certain extensions from a predetermined list, deleting all data contained in the targeted files. The ransomware payload differs from a standard ransomware attack in several ways, indicating a*

> *solely destructive intent.[12] However, later assessments indicate that damage was limited, likely a deliberate choice by the attackers.[11]*

There is another type of cyberattack called the **advanced persistent threat** (**APT**). This is a "stealthy threat actor, typically a nation state or state-sponsored group, which gains unauthorized access to a computer network and remains undetected for an extended period.[1][2]"

'Gamaredon' is such an APT of Russian origin which appears to have cyber espionage as its aim and has been operating since 2013. In January 2022 the group tried to attack a Western government entity in Ukraine. Besides attacking organisations in Ukraine, Gamaredon has targets all over the world.

Russia has various motives to use cyber weapons, including the spreading of disinformation, internet surveillance and persecution of cyber-dissidents.

Cyberwarfare by Russia - Wikipedia

> "An analysis by the Defense Intelligence Agency in 2017 outlines Russia's view of "Information Countermeasures" or IPb (*informatsionnoye protivoborstvo*) as "strategically decisive and critically important to control its domestic populace and influence adversary states", dividing 'Information Countermeasures' into two categories of "Informational-Technical" and "Informational-Psychological" groups. The former encompasses network operations relating to defense, attack, and exploitation and the latter to "attempts to change people's behavior or beliefs in favor of Russian governmental objectives."[3]

There were many cyber attacks before the 2014 invasion by Russia.

> *Main article: Russian-Ukrainian cyberwarfare*
>
> *In March 2014, a Russian cyber weapon called Snake or "Ouroboros" was reported to have created havoc on Ukrainian government systems.[40] The Snake tool kit began spreading into Ukrainian computer systems in 2010. It performed Computer Network Exploitation (CNE), as well as highly sophisticated Computer Network Attacks (CNA).[41]*

A Russian cyber espionage group is known to be associated with the Russian military intelligence agency (GRU).

Fancy Bear - Wikipedia:

> ***"Fancy Bear** (also known as **APT28** (by Mandiant), **Pawn Storm**, **Sofacy Group** (by Kaspersky), **Sednit**, **Tsar Team** (by FireEye) and **STRONTIUM** (by Microsoft))[2][4] is a Russian cyber espionage group. Cybersecurity firm CrowdStrike has said with a medium level of confidence that it is associated with the Russian military intelligence agency GRU.[5][6] The UK's Foreign and Commonwealth Office[7] as well as security firms SecureWorks,[8] ThreatConnect,[9] and Mandiant,[10] have also said the group is sponsored by the Russian government. In 2018, an indictment by the United States Special Counsel identified Fancy Bear as GRU **Unit 26165**.[3][2]"*

Fancy Bear hacked the Ukrainian Army's Rocket Forces and Artillery by an infected version of an Android app which targeted data for the D-30 Howitzer artillery. This particular app is used by Ukrainian officers and was distributed from 2014-2016. It contained X-Agent spyware, and was posted online on military forums. This program collects and transmits hacked files to servers operated by the hacker.

X-Agent - Wikipedia:

> *CrowdStrike claims the attack was successful, with more than 80% of Ukrainian D-30 Howitzers destroyed, the highest percentage loss of any artillery pieces in the army (a percentage that had never been previously reported and would mean the loss of nearly the entire arsenal of the biggest artillery piece of the Ukrainian Armed Forces.[42]).[43] According to*

the Ukrainian army, this number is incorrect and that losses in artillery weapons "were way below those reported" and that these losses "have nothing to do with the stated cause".[44]

Another attack on Ukraine:

The U.S. government concluded after a study that a cyber attack caused a power outage in Ukraine which left more than 200,000 people temporarily without power. The Russian hacking group Sandworm or the Russian government was possibly behind the malware attack on the Ukrainian power grid as well as a mining company and a large railway operator in December 2015.[45][46][47][48][49][50] A similar attack occurred in December 2016.[51]

In February 2021 Ukraine accused Russia of attacking the System of Electronic Interaction of Executive Bodies, a web portal used by the Ukrainian government to circulate documents by uploaded documents that contained macroscripts which, if downloaded and enabled, would lead to the computer to secretly download malware that would allow hackers to take over a computer.[52][53]

In January 2022, a cyberattack on Ukraine took down the website of the Ministry of Foreign Affairs and other government agencies.[54] Although an investigation has not been conclusive the cyber attacks coincide with the Russo-Ukrainian crisis.

In February 2022, before and after Russian troops entered eastern Ukraine amid an environment of escalating tensions between Ukraine and Russia, several major Ukrainian governmental and business websites were taken down by a series of cyberattacks. U.S. officials attributed the attacks to Russian attackers, although the Russian government denied involvement.[55]

2014 Ukrainian presidential election[edit]

Pro-Russian hackers launched a series of cyberattacks over several days to disrupt the May 2014 Ukrainian presidential election, releasing hacked emails, attempting to alter vote tallies, and delaying the final result with distributed denial-of-service (DDOS) attacks.[56][57] Malware that would have displayed a graphic declaring far-right candidate Dmytro Yarosh the electoral winner was removed from Ukraine's Central Election Commission less than an hour before polls closed. Despite this, Channel One Russia "reported that Mr. Yarosh had won and broadcast the fake graphic, citing the election commission's website, even though it had never appeared there."[56][58] According to Peter Ordeshook: "These faked results were geared for a specific audience in order to feed the Russian narrative that has claimed from the start that ultra-nationalists and Nazis were behind the revolution in Ukraine."[56]

Closing remarks

These are my conjectures:

As scientists, engineers, technologists and innovators usually do not have the power to determine how certain technologies are used, humanity is at the mercy of the decision makers especially the politicians. However, there are sophisticated technologies available to the public that can be used by civilians to join the battles to some extent. This possibly complicates the progress of wars, although it is as yet unclear how it influences outcomes.

Technology can be used for good or evil. It is the humans, and particularly the powerful, who mainly determine these uses. If ever it is possible to end war, the traits of human aggression and competition would have to change.

The available technology can determine the outcomes of war, and the side with access to the most sophisticated technology has a greater chance of winning. One could extrapolate that the side with the best access to education, ensuring the ability to use and invent sophisticated technologies, has the best chance of winning.

Scientists, engineers and other science professionals should stand up against the aggressors and advocate for the peaceful use of technology, and the fairness of its use for civilian purposes.

Further reading:

The cyber war between Ukraine and Russia: An overview | Reuters 10 May 2022

Senators seek boosts for JADC2, cyber mission, hypersonics in defense bill (defensenews.com) 17 June 2022

The Wargame Before the War: Russia Attacks Ukraine - War on the Rocks 2 March 2022

Treasury's Adeyemo sees elevated cyber threats in wake of Russia's war in Ukraine | Reuters

Ukraine War Attracts Belarusian Hackers in Fight vs. Putin - Bloomberg: A Ragtag Band of Hackers Is Waging Cyberwar on Putin's Supply Lines, 15 June 2022

Think of the Russia-Ukraine conflict as a microcosm of the cyber war (scmagazine.com) 17 June 2022

The opinions expressed above are those of the Executive Director, Ms Jansie Niehaus, and do not necessarily reflect the views of the Executive Committee or members of the NSTF.