



Technology and it's use in Terrorism

Note: Terrorism In-Action



Acts of violence seen as Terrorism:

In 1970's Brian Michael Jenkins said **"terrorism is theatre".**

Brenton Tarrant, 28 year old Australian shot 49 worshippers at two mosques in Christchurch. Broadcast live Facebook via helmet camera GoPro as the attacker welcomes his guest to the 'party'. As the live streaming of a French extremist knife murdering a policeman and his partner in 2016 on Facebook.

Manchester Arena, where 22 people died in May 2017

Suicide Bombings, 2018 Kabul and Nigeria

Stabbings in Russia 2018

Columbia Kidnapping and Assassination 2018

Hostage Taking and knife attacks in February 2019, Spain

Germany suffered shootings, assassinations in June of 2019

In Dallas, TX the shooting in June 17, 2019 at the courthouse

Stabbings on the London Bridge in November 2019, London, UK

4 chan distributes pornography

8chan hatred and extremist propaganda

Technology and it's use in Terrorism

Weapontry, Technology and Security

Historically, industry relied upon the technological advances as desirable involving weapons or explosives as defense uses. Time however, indicates this form of weapontry though not outdated by any means is no longer the prime influence upon technological advancement. We've been informed through media of the dated weapontry as society combats it's fears of access to guns and gun control mechanism are trifling through Congress as a means to implement such laws to minimize the impact upon lifespan they've been found to have. Though we are seemingly still faced with the urgency for the better and best available for those in security throughout the world in need of efficiency, lighter weight, and mobility. This has lead researchers into other and alternative facets of weapontry development as fighting in direct contact is not always the best means of control in the global effort to secure borders, safety of citizenry, and defense for other protected entities from forms of terror.

Let us digress into the world of global weapontry evolvement. Dynamite was patented in 1867 and automatic weapons became widespread after the Second World War. Rifles, shotguns, pistols, and automatic weapontry surfaced well after explosives having, through technological advance, improved for use in defense, and shear necessity for ease, transport and weight standards. Today, we are flooded globally with the assessibility of hightech guns for a gamet of uses as the arsenal units, gamers, hunters, and defense bodies are at a height for weapontry and manufacturers are readily competitive globally regarding design, material, and pricing.

Edit with WPS Office

a. corner shotguns [semi-automatic pistol/ grenade]

b. assault rifle [underwater use by Russian Special Forces]

c. Magpul FMG-9 [submachine gun folds up size of a laptop battery]

d. Armatix iP1 [finger print enabled]

e. Chiappa Rhino {Italian revolver]

These are forms of artillary which are specialized in usage and very expensive whereas only those willing to spend millions can readily distribute them for defense and trickle down for those with alternative motivation. Some have safety features which are believably able to deter needless, primative, and accidental shootings. Others are designed to use illusionary in the field manuevors on approach of assailants which preserves life as it indirectly reduces risk factors involved in war and criminal activity.

Afterwhich I note that chemical weapons had also evolved as the radicalization of 'nuclear energy' and it's ability in use to destroy entire continents prevailed as a deterant resulting in any aspect of its' value was downplayed sighting consideration toward humanity and life. This, however, did not cause a disconnection with the research and improvements for usage of other chemical aides for defensive means. Today our policing agencies are known to introduce 'riot control agents' RCA's upon civilians which are tear, vomiting, or malodents [unpleasant smells] chemical gases. Then there are the known 'nerve' altering agents which hender biological processes. Typically they cause blistering, choking or lung intoxication, and cyanides that cause partial or total incapacitation of those impacted from its use.

Now, well beyond these times, we find that the use of "Propaganda by deed" a 19th coined phase of terriorism is inset and ingrained in the character of some civilian outlets. It was well within 1950's and 60's that intellect taught us the use of radio and photojournalism to disseminate materials amongst those involved and caring for our sense of nationalism and security within this information age. That once assumed means of protection has long ago been violated and inundated with tribal, cultish, political, and other documented verbage more notable as forms of 'terroristic activity'. Early times it was to catch outlaws and common criminals. It circulates weather conditions or acts by the will of the forces of nature whereas today the use of media to distribute the messages of individuals or groups responsible for vicious acts across the globe. It supports the notion that these acts of 'Violence alone is not enough'. It is done to generate fear and change minds to mobilize the desire of such actors to enemies, supporters and those oblivious to it all.

Having technology within their reach, extremist have learned to exploit each new innovation online. Wheather live streaming apps or using encrypted messaging both are virulent forms of terrorism in their scope and reach. When media technology provides an outlet for this, it is much easier for the terrorist. One such instance was the onset use of 'satellite TV' which deregulated the news from the hands of editors and Arab regimes. It could be more loosely and directly released by fanaticalist and militants.This also meant that terrorist organizations were gaining ground and power as media corporations evolved. There were formal journalist and 'freelancer' aliken to terrorist groups respectively. So when the 'digital' forms of media network became heavily utilzed, independent channels created by such assumed terror groups reached their own audiences successfully. Most of these people are seeking 'witnesses or and audience' for their acts. Some believe God is sufficient and use 'dark' zones on the web attached by mainstream media. Their hope is to be viewed as a warrior, racial hero, leader and celebrity.

The realism of 'national security' mandates that safeguarding both domestic and international zones maintains there be a 'high alert' status. Those thought to be dangerous individuals modes of communication and their travel patterns are monitored. Proactively operants have technological tools at their descretion yet, there are alway 'blind' spots which escape their attention. They have sought to fill these gaps with alternatives to coincide with they existing systems.

Edit with WPS Office

As we twitter, view youtube videos, flicker and read from blogging platforms and other social networks so have they infiltrated these venues with videos, discreet messaging, 'dead dropping' emails to offset tracing. There is a continued mix of data transmitted in video games, cartoons, and children's programming.

Virtual chat rooms, forums, online forms of media, and the multitude of welcomed social net working platforms are all inundated with indirect transmission of terror group cultivation methods. There are plans for vicious acts encrypted messages protected via passwords or on software coded with materials for facilitating covert activities. Through the use of technology these bodies form and create global units with the financial means obtained illegally and legally as paypal charities, exploitation of online payment tools, use of others credit card numbers in identity theft schemes, wire, stock fund, or auction fraud. Intellectual property crimes and land development shell corporation are also still in great use. These are a some but not all of the manners monetary access is granted to such global terror organizations.

These groups target such sites as 4chan and 8chan to distribute their messages and generate live audience views of sexual, violent, and verbal acts to cause fear or gain followers who are equally as driven to disrupt life and penetrate homes with negative acts and information. White Supremacist, Neo-Nazism, and anti -semetism are primary thoughts and focal points we've come to be expectant of however, the Western World is full of sublets of networks who also share is spreading their form of hatred, racism and political opinions across these system networks and today it is shared in a timely and more fashionable means then the days of Osama Bin Laden.

Sites such as 8chan is attractive to those who radically incite the same negatism across the social climates throughout our countries. They annouced and carried many acts of hate, violence, and murders for all eyes to see as it gives them livesteam ability and a chance to dissiminate their perspectives while gaining their forum anonymously. Many have been caught for these life threatening acts but there is not resistance to distain for their interest.

The added use of 3D printing to fabricate homemade guns has caused a light stain across the progressive

At times, their fight involved simply destroying through usage of fire, cities and townships. Some of the noted battles such as, Battle of Ai with its devisive tactic in war groups to surround the kingdom, or the Assyrian siege on Jerusalem using a constructed water tunnel, have been depicted through filmwork and documentaries and reign in the minds of some as evil resignating in todays interpretations as biblical terror. Though a far-fetched notion to most, this opinion beyond the rims of religiosity are valid considerations amongst the intellecual circles.

When terroristic events happen in environments resembling our own, it always seems close as we see the images on our televisions, newspapers, phones and computers screens. In the wake of such danger, it has a constant beginning as information is disseminated amidst the confusion and chaos it generates. As reports are analyzed through commentators in successive time zones, identification of attackers, the victims, condolences, and other ritualistic acts are put forth as we debate the sense of such radicalism.

Today, around the world, these low tech terror attacks are common place as bombs, mass shootings, small scale attacks using objects such as cars, vans, knives, guns, as weapons supercede that of high advanced technological tools{satellite and laser usage}. However, western worldfears of Al -Qaeda and ISIS use of similiar means however, acquirering a greater level of weapontry is feared as ability to conjoin or gather monetary aide, through seizures, or hap happen stance, would bring about such discourse and the need to expose such risky potential outcomes is essential. Timid ownership and location of use might employ stronger security measures.

The internet bridges distances and borders circulating information within this dated cyberspace community. Having no continental boundaries, this technology is recognized as a fundamental human right to assure the sharing of information and ideas as it loudly enables digital media to spread world wide. With this no 'limitation' and subtle controls sense, propraganda from varied organizations, bodies or movements is easily distributed and thus the internets has became a great tools for recruitment, radicalization, generating means of financing, planning, and hence the execution of

Edit with WPS Office

But with this in mind the surgence of terror plots and the nature of such is changing. Traditional manifestation impose 'cells' with a network of co-sonspiritors spreading fear and destruction using extreme violence This envolve large monetary contributions and coordination which generally leave a trail of information.

The new nature is on individuals using low technology spastically and are harder to detect and interrupt. Less coordination as these are 'at will' acts being carried out. This exceeds the skills of standard security services. There is no 'plot' or trail to detect. Though in countries such as the U.K., camera surveillance is common mode of monitoring criminal activity. It caught the jogger being thrown into traffic, for instance from the reactive standpoint of use. Cameras are the option for gaining intelligence, however, it does not have predictory ability and can not be trusted as a reliable resource of information.

This makes it purposeful to implement use of 'Cognative radar technology' or intelligent video analytics systems which can identify weapons and explosives. Scanners will sit at chokepoints for laptop, tablet, or phone threats. This reduces the 'policing' burden as it constantly monitors for visible and concealed threats in the form of large weapons, vest, explosive and other catalogued threat items. This imploys the use of 'algorithms to identify threats and it ability to removed bias and pre-conceptions in use. It is believed to be a means of eliminating 'racial profiling'. Yet it is said to depend upon the 'technical written [content]' ability of the algorithm itself. All of this technology is committed to an integrted platfom which connects all options to headquarters. This will enhance and modernize most security systems.

Forms of Terror and Technology

It is becoming a common incentive for cultural exploration to renounce the use of biblical text having documented terror historically as it is recognized in the days and date where foreign nations are noted as having supported terrioristic bodies in times of descent. The battles fought against these nations speared well devised attacks with such synchronizing to implode terror through

It is quick and cost effective enabling the production over a simple weekend at the low material price of $50. The guidelines for such at home manufacturing of 'guns' is readily accesssible over the internet also and has been for quite some time. It has minimum usage abilit however, the slight impact is still that of uncontrollable violence and a safety issue for society at large. Especially to be considered as an viable option in countries where 'gun controls' are firmly in place. As the quality and techniques of 3D production improve so grows the risk and effectiveness of terrorist making these devices.

Public and private partnerships, as in Facebook, Google, Microsoft etc....., serve as mediums between the technological advancements and the distribution and for -use indicators by authorities and experts of both aspects of our business and policing bodies. As such companies can and are more willing to be in the position to remove means of cummunication, channels or website which contribute to the distribution of inappropriate materials and information as deemed so by their collective sense. It is a complex trigger which must be implemented to protect users and mand/abide by the laws of each country as a duality of such.

Cyber- Terrorism

Technology and time find use subcombing to modern forms of internet terrorism as acts of cyber terrorism, cybercrime, or hacktivism are typically relative to social, religious, economic, political or cultural activism. They are readily identified in term relative vocabulary those of us outside of the industry must learn:

a. Phising: fraudulent emails to convence target of the legitimacy of a user or organization in order to obtain private information

b. WaterHole: deployment of a fake webpage to compromise the original in oeder to attack
visiting users

c. Ransomware: infecting a system by encrypting files and or locking the users access to said system

d. Scanning: testing your vunerbility in specfic files and or locking the users access to said system



Edit with WPS Office

Cyber Targeted Attacks:

a. spear-phishing targets individuals ororganization

b. distributed denial or service: deploy mass amts of packet request to 1 website or network in order to overload the system and prevent regular access by legitamate users

c. supply chain: attacking an element of an organization before it arrives

d. Zero-day: bespoke exploitation of a system with specific vulnerable aspect not yet known to the author

e. Dyn Attacks are typically geared for Name Servers , DDoS upset web addresses and prevent them from coming up. These hackers sneak in undetected Greeks using a Trojan Horse. In 2014, Yahoo found a 'slow' leak of it's data. This has been the repeated suffrage of corporations who are knowledgeable of their vulnerable states against hackers and those implementing terroristic cyber attacks to gain results aligning with their interest. This will continues as their efforts to terrorize, equate to other professionals, or seek a form of revenge is a constant within the world we live and thrive in.

Identified Potential Threats:

a. generater fire: turbines set afire

b. hacker controlled "ICS" that operated the flow of natural gas increasing it until valve breaks and an explosion

c. unfrastructure and internet services to disrupt companies and governments opposing beliefs

Measure being pursued in prevention as the digital infrastructure of our nations are under constant watch for vulnerbilities. Research exposed threats posed by new technology within the defense and security sectors and how it can indirectly come into usage in places of the western world and The Netherlands.



Security, AI Fantasy and Smart Cities Designs

There currently exist no known autonomous targeting systems with out human decisions making employed in the (US) military. One known guideline is to ALWAYS have a human in the loop. However, it is known that some of the countries developing and using the technology are feared to disregard the same standards and fundamental framework which accounts for individual liberties and rights. China is a known user of 'facial recognition' software for mass surveil. Other 'unknown' countries may also use such security software. A 2019 report suggest 75 of 176 countries are active users. One such is that of The Netherlands. This confirms that AI technology is sold to and used by fragile and instable states. These fragile territories are of great consideration as any collapse or conflict can plausibly lead to militant groups or terrorist organizations acquiring such property intensifying global threats.

Youtube and other online video sites with high volume viewership are outlets of distribution for activist groups of any kind. For example, the proliferation of Slaughterbots 2017 video generated believability in these dynamic systems of defense which have been said to falsely portray such technological ability. These techies suggest that a all inclusive device using facial recognition, explosives, the algorithms and drone technology have bee developed but different in context then the governmental versions which are not considered consumer goods. They are weaponized drones to kill 'critical' civilians. However is has been formally noted that there are means by which to 'counter' measures against drone activity such as simple use of chicken wire and nets.

Evidence through scenario development as to the assumptive use of AI and Killer drones is how best to devise mechanisms to counter such actions. Using our imagination to project plausible incentives and motivations researchers pose a 'threat assessments' of technical capabilities and unhindered access to these new devices, AI-robots, killer robots with the capacities that mimic that of the human brain are new. Here, we can attribute "homo-sapiens' with having the decency and morality not to committ assassinations the way AI robots would. As they are impartial to 'sensory' and designed to 'operate' thy do not have

Edit with WPS Office

Usage of self-sacrificed human operatives is fanaticism which strengthens their image as victors [super heroes of sort] and up-grade the impact of such security real life outlets. The reality is the authorization on 'terror' do not anticipate AI powered opeatives to carry out assassinations or attacks nor self-driving vehicles carrying car bombs or ramming attacks. The governmental initiatives security and securing perimeters states not terrorist.

Governments are faced with finding a way to strike a balance, and a covert, multi-sensor platform approach to threat detection. This poses as a rational solution. Most major cities are experimenting with implementing these 'intelligent' systems to improve their policing, community outreach, and urban safety. It is incorporated in the 'smart city' initiatives. These are termed 'agile security' as it's computing power and machine learning ability which speeds up data processing relative to crime and terrorism to identify correlations and causes. It can relay real time data by use of crime mapping platforms, gunshot detection systems, CCTVs or smart lights to detect crime before it happens. These systems are deep neural networks connected to the cloud for access license plates, facial recognition software etc....are incorporated for swift service of policing bodies. The use of 'fusion' centres to stream multiple datasets from a wide range of sources with in city sensors zone and cybercrime units in private companies is problematic. As they are for counter-terrorism and emergency responser agency's they are still issues of privacy for citizens.

Urban plans of these cities is also a means of controlling crime by 'designing out' threats of crime and terrorism in building structures [low], making physical changes to the environment, promoting mixed communities, and renewal measures in disadvantaged neighborhoods. Investing in high-quality public goods and social inclusion can help prevent crime and radicalization. City leadership must find a means to consult their community residents to discuss these motives and the implications of such new technology being utilized as it impacts civil liberties both intentionally and unintentionally. A criteria should be established to personal data access, retention and redress. This can create a loss in confidence and support of law enforcement as it stresses the social distance

Yet, the protectionist implore camera video surveillance to produce evidence of disobedience and as a means of stifling land access cyber crimes, cloud walk technology is used for mining personal data and profile high risk individuals. There will never be 100% but more accurately placed at a 50% rate in securing cyber-data as the response of 'human nature' and data flow flaws are evident and lend toward invading public privacy. Hence, it is decided that privacy is non-existent as we discuss such conditions in vicious feedback loops globally disputing the security principles and procedures the public is subjected and resistant to.

Preventive Measures

Because of the difficulty associated with survival such cyberattacks, the administrative technologist have strengthened interest in protecting and prevention of the wide range of technologic systems privey to plausible terrorist inaction. Ungrading and redefinement of security measures and programs is a constant amongst the research and development units globally. Typical firewalls, passwords, key encryptions, protection systems and intruder detection systems in IP security and access control list are in place but so are those individuals and teams which labor in creating means and bugs to uproute the functionality of these system and programs.

The tryst mentality for preserving data during an attack is punctured in understanding where vulnerbilities exist and cyber attack may occur. Generating a method to indentify points and places of attack is as essential as tracing elements to locate these intruders. Some companies feature 'fire drill' procedures in how staff can best address such situations when they arise. This is reiterated in education tools for both the public and private sectors.

Investigations Into Global Cyber Criminal Activities

No investigation can move forward without the counter interest into the in-house actions of Corporate employees well before and during a search for external hackers. There could always

Edit with WPS Office

The attraction of cyber bugs can potentially be from attempts to breach firewalls as an employees 'scope of duties' has implied limitations. This is should be an initial investigative stage resolutive resource.

Investigations and prosecutions of cases involving digital evidence requires specialist criminal investigative skills and expertise. These are typically 'forensic' specialist for data preservation and recovery. Some countries policing agencies are not equiped technologically and lack the valued manpower to conduct such investigations. Yet these are criminal acts severe in outcome and warranting proper enforcement. Hence, there is a need for familiarity with the legal and procedural requirements to establish admissibility for both purposes of domestic and international investigations. The cyber and technology laws hold international variance which signify's the necessity to become versed as professionals with State egal processes and recognize the urgency to stipulate with investigative teams the need for 'clear chain of custody' of any evidence from the time it is first secured to eleviate plausibility of tampering from moment of seizure until it is produced in court.

There can be selective standards of categoric forensic data recovered from 'electronic communications'. It can and issue of IP's which denote the region or state a computer connecting or is currently connecting from or the access to the RAM data from a hard drive. This information can be irretrievably lost however, it some form of power supply outage disrupts the device. Electronic mail is a resource for providing messages through the use of shared passwords and 'drafts' of messages transmitting coded information anonymously. The envelop header should contain a record of each mail server the message transited on the way to it's recipient. This is the key investigative means of international cooperaive and specialized investigations. As this data may not be recoverable from servers or chat room shared information after the device session has been terminated, it can be retrieved with forensic analysis of a participants hard drive and without the ability to suggested any sense of 'entrapment' from authorities.

There are some file sharing networks transfer logs or payment information which has been compromised as the 'cloud' technology has come into full use. This data first is widely distributed and remotely stored

This holds true for 'at-rest' data on flash media, smart devices, in transit data, etc.... In the United Kingdom, it is considered a criminal offense under the 'Regulation of Investigatory Powers Act 2000' to refuse to hand over an encryption 'key' when required by authorities. In the U.S., similiar standards have been applied by law for material confiscation whereas in places such as Belgium, self-incrimination is eliminated as law only allows for law enforcement to compel assistance from non-suspects and in some countries law is specific to third parties only.

The use of Vocal matter using voice over internet, video chat, or textchat, skyping are also use low bandwidth transfer as this is difficult for law enforcement authorities to corroborate authenticity of communication and make it evidence in legal cases. Even wifi 'hotspots' are violated and function as monitored and searched in crimes. This too is a privacy violation and problem oriented policing practice.

Future of Law Enforcement

Research and Development always plays a role in securing the ability to implicate protectionism while advocating usage of technology devices. The roles of those educating and functioning through the world as 'technologist' offers and affords them the option of interest in safe guarding this evolving industry. In Dublin, on such institution is developing program software focused in forensic investigative processes which assist undersourced cybercrime units with limited budgest and personnel in management of their case loads. They've created 'open' source forensics lab that instructs on building computer evidence, storage procedures and processing equipment required.

Education Forum:

Youtube: Hot Robot At SXSW Says She Wants To Destroy Humans The Pulse [Sophia]

Robot Humanoid Tells Jokes on Good Morning Britain

Black Mirror [netflix]

Bible Battles [youtube]

Edit with WPS Office

Legal Justification as Technological Crimes

The legal aspects of Terrorist Protection are implemented as '*softlaws*' which are the primary source of political commitments or emerging norms of international law which are 'universal' legal instruments as agreements that open for ratification or accession by all 'Member States' of the United Nations.

Articles 15 and 19 of International Covenant on Civil and Political Rights also grant the ability to prosecute or gain global assitance depending upon the 'stated' laws of each affected countries by the terror cyber act.

The *Rule of Law* considerations suggest states have a right and a duty to take effective measures to counter the destructive impact of terrorism on human rights and particular rights to life, liberty and physical integrity of individuals and the territorial integrity and security of states.

Insurance For Cybercrimes

The regulation of cyber insurance peaked in 2017 as a tool of and for consumer resolution in times of destructive technological devise. It is suitable for those interested in the 'best' practices against an industry with a shortage of cyber security experts, having high insurance premiums, and a insufficient automated security enforcement system.

References:

Amazon. Seattle Times.com: How technology is improving disaster relief. Jan 3, 2020

Burke, Jason. theguardian.com: Technology is terriorism's most effective ally. It delivers a global audience webarticle

Brookings Institute: Global Research Network on Terrorism and Technology: The inaugural conference. 2019 May. webarticle

Clingendael.org RESEARCH / STRATEGIC FORESIGHT / REPORTS AND PAPERS

Cronin, Martin. defenceig.com: Proactive vs. reactive security: How technology can improve counter terrorism. Cognitive radar technology or intelligent video analytics systems can be deployed to indentify weapons and explosives. 05/31/2019

Harwell, Drew. The Washington Post: El Paso Massacre, August 4 2019 racist manifesto and the annoucement of the anonymous message board of 8chan of the coming web-fueled racist bloodshed.

Ismail, Nick. The Trojan horse: cyber security trends in 2017 cybersecurity. 18 November 2016

Littl3field. CyberTerrorism: understanding and preventing acts of terror within our cyberspace. June 7 2017

Muggah, Robert. SecDevGroup: How smart tech helps cities fight terrorism and crime. 15 Jun 2018

nap.edu / protecting individual privacy in the struggle against terrorist a framework

TERRORISM IN THE AGE OF TECHNOLOGY 04 DEC 2019 online report

UNODC [United Nations office on Drugs and Crime]: The use of the Internet For Terroist Purposes: In collaboration with the United Nations Counter-Terrorism Implementation Task Force. September 2012

Edit with WPS Office

Edit with WPS Office