Introduction

Technology is advancing at such a rapid pace that it is becoming increasingly difficult to assess the safety and efficacy of each technology before implementation. Furthermore, regulatory oversight and the law, which traditionally lag in regard to technology, are slipping even further behind this wave of technological development. New technologies that are disruptive, untested and not well-established are referred to as emerging. There are many different ways to define an emerging technology, but in general, an emerging technology is one that has the capacity to change the status quo. No matter the definition, all emerging technologies share five key attributes as defined by D. Rotolo:

- Radical novelty
- Relatively fast growth
- Coherence
- Prominent impact
- Uncertainty and ambiguity [1]

It is really the combination of these attributes that not only makes an emerging technology so attractive for positive, societal change, but also generates an environment for potential concern. Apart from environmental, health and safety issues, the concept of emerging technologies has generated apprehension and in some cases fear among military leaders and security experts. NATO has evaluated the impact of emerging technologies on arms control, [2] and a review of U.S. Naval strategy warned that the impact of emerging technologies on mission capabilities is ambiguous. [3] In fact, the latest U.S. National Military Strategy goes as far to state that, “emerging technologies are impacting the calculus of deterrence and conflict management by in-
creasing uncertainty and compressing decision space." [4]

The possibilities of nefarious use and security breaches emanating from emerging technologies have always been cause for alarm. In fact, some of the most notable technological developments in the 20th century (which were emerging in their time) still plague us today: nuclear fission, the internet and rocketry. These technologies have not just opened us up to new worlds of energy production, communication and travel, but also created fear and panic related to the advent of nuclear weapons, social media propaganda and cyber threats.

The Possibilities for New Threats

Each year the World Economic Forum releases a list of the top 10 emerging technologies to watch for during the upcoming year. Over the past five years, six key groups of technologies are emerging as the most prominent (See Table 1) and are represented in Figure 1.

Aside from being new and not well-established, the aura surrounding many of these technologies is further complicated by the fact that they are considered dual-use technologies, meaning that most legitimate and beneficial uses of the technologies also brings a darker, more sinister application. The challenges associated with dual-use technologies are threefold:

• **Complexity** – Many variables with unknown or unknowable consequences
• **Uncertainty** – Inability to produce usable risk versus benefit assessments
• **Ambiguity** – Often involve conflicts over ethical and professional values

Many of these technologies, if not all, are also being utilized by militaries for use in weapons systems, leading to a resurgence in not only proliferation but state-sponsored
scientific research programs that often are used to drive militarization.

The emergence of new technologies, their expected use in military and terror tactics, and a general unawareness of potential consequences has created a new class of security risks that could defy countermeasures used for more classical types of threats, such as nuclear weapons. Nontraditional risks associated with technological innovation can be classified as emerging security challenges and may defy established security agendas. [12] Examples of risks associated with the emerging technologies described earlier can be found in Table 2. These technologies are the most rapidly developing and pervasive, and the potential risks they bring deserve further attention.

**Intellectual Property Theft and Espionage**

Theft of intellectual property and espionage are not new crimes; however, the type of information that is being smuggled or potentially stolen is changing all the time. As emerging technologies develop and evolve, the allure they bring in terms of competitive advantage and innovation will become more sought-after, and their value will bring big rewards from some and great loss for others.

In 2014, Jianyu Huang, a former scientist at the Department of Energy pleaded guilty to making a false statement and unlawfully transporting converted government property in interstate and foreign commerce. Huang, a naturalized U.S. citizen from China, was employed at the Center for Integrated Nanotechnologies, which is a user facility jointly operated by Sandia National Laboratories and Los Alamos National Laboratory. From 2009 to 2012, Huang made a series of trips to China in which he brought his government issued laptop containing sensitive information regarding his research with him. He admitted to sharing the information on this laptop with businesses and universities throughout China and was sentenced to one year in prison. [13]

Five men in Taiwan were charged in July 2016 with stealing intellectual property from a nanotechnology company and setting up competing nanotechnology plants in China. The men are former employees of Hsin Fang Nano Technology Co., which developed a novel process for manufacturing nanopowders used in a variety of applications. The men used the information they stole to create Unicat Nan Advanced Materials & Devices Technology Co., and operated it successfully for several years before being apprehended. The estimated financial loss to Hsin Fang is reported to be approximately $82 million U.S. dollars and cost the company 15 years of research. [14]

Apart from nanotechnology, other technologies, such as 3D printing and synthetic biology, pose new risks to IP, particularly in the patenting aspect. Two things are needed to operate a 3D printer: material and a design. The material is either a polymer composite or a metal, and the design is an electronic file (computer-aided design file) that can be developed on special software and even downloaded from the internet. Traditionally, product design has been protected because

<table>
<thead>
<tr>
<th>Technology Area</th>
<th>2012</th>
<th>2013</th>
<th>2014</th>
<th>2015</th>
<th>2016</th>
</tr>
</thead>
<tbody>
<tr>
<td>Informatics for Adding Value to Information</td>
<td>OnLine Electric Vehicles</td>
<td>Wearable Electronics</td>
<td>Fuel Cell Vehicles</td>
<td>Nanosensors and the Internet of Things</td>
<td></td>
</tr>
<tr>
<td>Synthetic Biology and Metabolic Engineering</td>
<td>3-D Printing and Remote Manufacturing</td>
<td>Screenless Display</td>
<td>Next-generation Robotics</td>
<td>Next Generation Batteries</td>
<td></td>
</tr>
<tr>
<td>Green Revolution 2.0 – Technologies for Increased Food and Biomass</td>
<td>Self-healing Materials</td>
<td>Human Microbiome Therapeutics</td>
<td>Recyclable Thermoset Plastics</td>
<td>The Blockchain</td>
<td></td>
</tr>
<tr>
<td>Nanoscale Design of Materials</td>
<td>Energy-efficient Water Purification</td>
<td>RNA-based Therapeutics</td>
<td>Precise Genetic-engineering</td>
<td>2D Materials</td>
<td></td>
</tr>
<tr>
<td>Systems Biology and Computational Modelling/Simulation of chemical and Biological Systems</td>
<td>Carbon Dioxide (CO2) Conversion and Use</td>
<td>Quantified Self (Predictive Analytics)</td>
<td>Additive Manufacturing</td>
<td>Autonomous Vehicles</td>
<td></td>
</tr>
<tr>
<td>Utilization of Carbon Dioxide as a Resource</td>
<td>Enhanced nutrition to Drive Health at the Molecular Level</td>
<td>Brain-computer Interfaces</td>
<td>Emergent Artificial Intelligence</td>
<td>Organs-on-Chips</td>
<td></td>
</tr>
<tr>
<td>Wireless Power</td>
<td>Remote Sensing</td>
<td>Nanostructured Carbon</td>
<td>Distributed Manufacturing</td>
<td>Perovskite Solar Cells</td>
<td></td>
</tr>
<tr>
<td>High Energy Density Power Systems</td>
<td>Precise Drug Delivery through Nanoscale Engineering</td>
<td>Mining from Desalination Brine</td>
<td>“Sense and Avoid” Drones</td>
<td>Open AI Ecosystem</td>
<td></td>
</tr>
<tr>
<td>Personalized Medicine, Nutrition and Disease Prevention</td>
<td>Organic electronics and Photovoltaics</td>
<td>Grid-scale Electricity Storage</td>
<td>Neuromorphic Technology</td>
<td>Optogenetics</td>
<td></td>
</tr>
<tr>
<td>Enhanced Education Technology</td>
<td>Fourth-generation reactors and Nuclear Waste Recycling</td>
<td>Nanowire Lithium-ion Batteries</td>
<td>Digital Genome</td>
<td>Systems Metabolic Engineering</td>
<td></td>
</tr>
</tbody>
</table>

Table 1: The World Economic Forum’s Top 10 Emerging Technologies by year for 2012-2016 with technologies representative of six key groups. (Released) [58,59,60,61,62]
only the manufacturer has the specifications and the ability to create the item; however, 3D printers are changing that model. The cost of a small 3D printer is only a few hundred dollars, and because CAD files are digital, they can be shared across the internet on file-sharing services, just like movies and music. [15] It is now possible for someone to find the plan online for a product they want to create and simply download and print it on a desktop 3D printer at home.

Somewhat more complex, but maybe even more alarming, is the possibility of patent wars for biological innovations. In 2013, the U.S. Supreme Court ruled in Association for Molecular Pathology et al. v. Myriad Genetics that human genes are not patentable but synthetic DNA is patent eligible because it does not occur in nature. [16] Although this ruling puts limitations on developments in biotechnology related to gene-sequencing, this ruling opens up many new possibilities including a potential war for creating new organisms and being the first to market in order to reap the financial rewards.

Loss of Control and Sabotage

The connectivity of items to the internet, and the expanded use of electronics and code in general has created a new venue for causing damage and destruction. Sabotage may be one of the oldest threats known to humanity, but technology is opening up the possibility to do this in completely new ways. One example is through 3D printers that are connected to the internet, allowing for remote control. Hackers might be able to target these printers and secretly introduce catastrophic internal defects in the manufacturing process, change the printing orientation or insert fine defects that may manifest at a later time. [17] This may not seem to be a huge concern until the extreme consequences are truly realized. Imagine that thousands of parts used in engines and airplanes are covertly altered and unknowingly placed into service, only to fail at some later time during operation leading to unexplained multiple crashes at once. This is becoming more of a likely scenario as industrial 3D printing becomes more of a widespread reality. [18] These fears apply even to medicine. In August 2015, Aprecia Pharmaceuticals received Food and Drug Administration approval for the first 3D printed drug, Spritam (levetiracetam), which is used to control seizures brought on by epilepsy. [19,20] If the files that drive the printing of the pills were altered in any way, the entire dosing and effectiveness could be manipulated and would potentially compromise the health of anyone taking the drug.

Looking beyond 3D printing, connectivity in general has generated new ways of wreaking havoc on systems. In October 2016, a large portion of the internet was threatened when hackers used the IoT to execute a distributed denial of service attack. [18] A DDoS occurs when a machine receives so many commands that it crashes because it cannot keep up. What is interesting in this case is that hackers utilized something called a “Mirai” botnet that specifically targeted internet-connected devices resulting in more than 500,000 devices being comprised and sending out signals simultaneously and bringing down part of the internet. [21]

More than household devices are connected to the internet. Many aspects of critical infrastructure, such as power plants and dams, are connected to the internet to provide remote and automated access in order to improve the efficiency of operations and reduce the amount of hours a person needs to spend on-site. While this aspect of connectivity does improve operational capacity, for obvious reasons, it creates security threats. For example, sensors are often placed on dams in order to measure water levels and automatically control flood gates if the height of water in the reservoir changes. It is possible to manipulate the sensors and cause the dam’s system to think that the levels are too high (a process called spoofing) and open the flood gates leading to multiple unexplained crashes at once. This is becoming more of a likely scenario as industrial 3D printing becomes more of a widespread reality. [18] These fears apply even to medicine. In August 2015, Aprecia Pharmaceuticals received Food and

<table>
<thead>
<tr>
<th>Risks</th>
<th>Technologies</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>Intellectual property theft/espionage</td>
<td>• 3D printing</td>
<td>• Copyright infringement</td>
</tr>
<tr>
<td></td>
<td>• Biotechnology</td>
<td>• Security vulnerabilities</td>
</tr>
<tr>
<td></td>
<td>• Nanotechnology</td>
<td>• Financial loss</td>
</tr>
<tr>
<td></td>
<td>• Synthetic biology</td>
<td>• Patent wars</td>
</tr>
<tr>
<td>Loss of control/sabotage</td>
<td>• Artificial intelligence</td>
<td>• Rogue unmanned systems</td>
</tr>
<tr>
<td></td>
<td>• Internet of things</td>
<td>• Spoofing</td>
</tr>
<tr>
<td>Terrorism/WMD</td>
<td>• 3D printing</td>
<td>• Untraceable weapons</td>
</tr>
<tr>
<td></td>
<td>• Biotechnology</td>
<td>• Genetically altered diseases</td>
</tr>
<tr>
<td></td>
<td>• Internet of things</td>
<td>• Hostile control</td>
</tr>
<tr>
<td></td>
<td>• Nanotechnology</td>
<td>• Unidentifiable poisons</td>
</tr>
<tr>
<td></td>
<td>• Synthetic biology</td>
<td>• Untreatable illnesses</td>
</tr>
</tbody>
</table>

Table 2: Key emerging technologies, their associated risks, and some examples of concerns. (Released)
ing to an unplanned and potentially catastrophic release. A group of Iranian hackers gained access to the Bowman Dam in Rye, New York, in 2013. [22] They never gained access to the dam itself, but they did learn information about how the flood gates are controlled.

Artificial intelligence is creating a unique set of risks, in particular one that has frightened humanity for decades, and that is the threat of machines taking over. While the threat may not necessarily be imminent, there is some cause for alarm as both the private sector and the militaries of many nations push to have more autonomous and intelligent machines. In an effort to keep tabs on the activities of semi-autonomous and even autonomous systems, the Department of Defense released DoD Directive 3000.09 prohibiting the creation or use of unmanned systems to, "select and engage individual targets or specific target groups that have not been previously selected by an authorized human operator." [23] This sort of protection becomes imperative when looking at a weapons platform such as the South Korean Super aEgis II, which is the first weapon system capable of recognizing and targeting humans. [24] However, the nature of machine learning in intelligent systems would eventually enable a system to figure out how to get around this failsafe, [25] and at some point, the human would be removed from the equation altogether. Google’s Brain deep learning project developed three neural networks named Alice, Bob and Eve that passed each other notes using an encryption method they created themselves. [26] This is the first AI-generated, human-independent encryption.

Understanding what it would mean if a human were unable to gain or regain control of an autonomous, semi-autonomous or intelligent system is the sort of scenario that is becoming more likely. [27,28] "We believe strongly that humans should be the only ones to decide when to use lethal force. But when you’re under attack, especially at machine speeds, we want to have a machine that can protect us," Deputy Defense Secretary Robert Work said. [29] In fact, this type of response has already been demonstrated as an AI-controlled drone defeated a pilot in a simulated dogfight. [30]

As the DoD continues to develop its Third Offset Strategy [31] and push for more autonomous systems in which humans play a vital role, but not necessarily the lead role, preparing for risks, such as losing control through hacking or intrinsic systems design, will be paramount. Additionally, preparing for attacks from intelligent systems that do not have the same “human in the loop” safeguards will be equally important.

### Terrorism and Weapons of Mass Destruction

In 1346, a Tartar (a subjugated peoples of the Mongol Empire) army laid siege to the city of Caffa on the Crimean peninsula. Sometime after the siege began, the Tartars were stricken with an outbreak of the plague. As the body count mounted, the Tartar commander decided to change the rules of the game and ordered plague-infected corpses to be catapulted into the city. Shortly after, an outbreak of plague erupted inside the walls of Caffa. This event is long believed to have initiated the Black Death that killed one-fourth to one-third of Europe’s population in the 14th century. [32]

In 1978, a Bulgarian dissident named Georgie Markov was attacked with an umbrella in London. Unbeknownst to Markov, the umbrella was modified and used to inject a pellet containing ricin into his leg. Ricin is a highly toxic substance found in the castor bean. He died four days after the attack. [33]

In November 2006, a healthy man was admitted into a London hospital with severe gastrointestinal symptoms. He died approximately three weeks later. His death was later determined to be caused by poisoning from Polonium-210, a radioactive substance. [34]

The connection between all three of these events is that they are the first of their kind. No one ever thought these things could or would happen until they did. In many ways, these incidents set the precedent for what it means to be prepared to face emerging security risks. The emerging technologies discussed throughout have the potential to be used as new weapons of terror.
One of the hallmarks of emerging technologies is the uncertainty they naturally harbor, which for obvious reasons, poses unique challenges in preventing attacks as evidenced by a strange report from Russia. Svetlana Zheludeva, a deputy director at the Russian Academy of Sciences, died suddenly after opening a letter containing a white powder. The sender of the letter had sent several similar letters with the white powder to other scientists claiming the powder was a product of his research in nanotechnology; however, no other recipients of the letters died, and test results supposedly showed that the powder was ordinary quartz sand. Russian authorities have stated that there will be no criminal charges and no other information about the case is available. [35]

Even more concerning than bizarre nanotechnology case reports are real instances of biotechnology and synthetic biology used to create more virulent organisms, and, in some cases, completely new ones. A report prepared by the United Nations Interregional Crime and Justice Research Institute called attention to the possibility that beneficial applications of synthetic biology and biotechnology could be suitable for use as enhanced biological weapons and used by criminals or terrorist. [36] Gene editing techniques, such as clustered regularly-interspaced short palindromic repeats, have the potential to revolutionize medical treatments by altering faulty genes in patients suffering from rare or degenerative disorders; [37] however, CRISPR could also be used to create mutated strains of organisms that could be lethal, and, in fact, CRISPR has already been used to modify human embryos. [38]

Over the past decade and a half, researchers have used genetic engineering techniques to develop hypervirulent strains of viruses in an effort to use that information to create more efficacious vaccines. However, the development of these new viruses and the debate as to whether or not the results of this research should be published openly has created ethical and security challenges. To date, some of the more important biotechnology research includes:

- 100 percent fatal strains of mouse pox created [39,40]
- Genetic characterization of the 1918 influenza pandemic (H1N1) [41]
- Genomic characterization of the Plague that destroyed Europe in the 14th century [42]
- More virulent strain of bird flu (H5N1) engineered [43,44]
- Recreation of 1918 influenza strain (H1N1) using various strains of bird flu (H5N1) [45]

In September 2016 researchers in the United Kingdom created the world’s smallest virus, measuring 12 nm in diameter. [46] This was unprecedented considering this was the first artificial virus ever created, but it also opens up a new possibility for biological warfare. No longer does military or terrorist organizations have to aerosolize existing organisms; they can now create them. These artificial viruses have no known treatments since they have never existed before, which creates new challenges to developing countermeasures and anticipating threats.

Aside from chem-bio attacks, emerging technologies are changing the landscape for how traditional attacks could be carried out. The first 3D printed weapon was successfully fired in 2013, [47] and in August 2016, Transportation Security Administration officers at the Reno, Nevada, airport confiscated a loaded 3D printed handgun in a passenger carry-on bag. [48] More interesting is the fact that the U.S. military has an interest in new 3D printing technology that would allow soldiers in the field to potentially print entire missiles at once. [49] A platform like this could be a game-changer for terrorist organizations in terms of leveling the playing field regarding weapons production and availability.

Finally, new technologies not only bring risk through the potential of creating new types of weapons but the concept of the technology itself poses a threat. Since the early 2000s, a series of attacks and protests aimed at nanotechnology-themed activities and research centers has occurred across the world (Table 3). In many cases, these were harmless protests incited by students or local environmental groups. However, a failed attack on the IBM facility in Zurich and several planned attacks throughout Mexico were orchestrated by known terrorist organizations, and possibly connected to a group known as the Olga Cell, part of an Italian-based internal terrorist organization known as the Federaziona Anarchia Informale. [50]

Part of the challenge to managing emerging technologies is anticipating what, if anything, could potentially go wrong. The other aspect is to understand what to do in order to manage the fallout of an adverse event. Typically, policy and the rule of law is how most threats are mitigated. In fact, legislators and regulators have looked at existing legal frameworks in order to control emerging threats from technologies. In terms of nanotechnology, biotechnology and synthetic biology, chemical and biological weapons bans and treaties have been deemed appropriate to control the proliferation of new threats. However, biological innovations have always seemed to garner more attention than others, starting with the Ansilomar Conference in 1975 [51] and culminating with the recent announcement of the intent by the National Academy of Sciences and the DoD’s Office of the Deputy Assistant Secretary of Defense, Chemical and Biological Defense to assess biodefense given new advances in synthetic biology. [52]

The big problem is that laws are only as good as the people who choose to follow them. The key issue is how to mitigate threats of emerging technologies in the face of any and all environments. Foremost is promoting awareness of not only emerging technologies, but the potential and actual risks they invoke, particularly as everyone, including rogue states and violent non-state actors, are gaining access to the same technology. [52] Recommendations for addressing risks of emerging technologies revolve around awareness, social responsibility and research:
Increase awareness of the dual role of emerging technologies and their unintended security consequences

Identify and address emerging security concerns now, even if the threat seems to be remote

Build emerging security concerns into education curricula and have it addressed within national institutions

More dialogue around risk governance priorities between industry, academia, and government

Increase funding and priority for research related to risk governance

Promote a culture of responsibility around innovation

Include applications of technology in war gaming scenarios used to train military leaders [52,53,54]

Some of these recommendations are already in practice. The FBI launched a program to identify suspicious activity that could be connected to nefarious uses of synthetic biology. The Synthetic Biology Tripwire Initiative is a system in which suppliers of biological products used in synthetic biology or biotechnology alert the FBI when odd requests are made. [55] DARPA announced in September 2016 that it was developing Safe Genes, a program to develop a set of tools used to address potential risks of gene editing. [56] UNICRI is in the process of opening the Center for Artificial Intelligence and Robotics, aimed at raising awareness of the risks and benefits of AI. [57] While these initiatives are a good start, more focus needs to be put on other technologies and include training for first responders.

Conclusion

In many ways, the title of this article may be misleading. These are not necessarily new risks, but rather relatively common risks that are brought about in ways that have not been used before. However, the fact that most of the world is unprepared to mitigate any one of these scenarios, let alone facing the possibility of several of these scenarios occurring at once, is disconcerting, to say the least. If the 20th century taught us anything, it is that science and technology can be both our greatest friend and our worst enemy. Few people want to think about the impossible or the unknowable, let alone spend money preparing for something that may or may not happen. However, it is always better to plan because each of the events in this article have happened, and these are just the ones we know about.

References

2. Special Report: Emerging Technologies and Their Impact on Arms Control and Non-Proliferation, Nato Parliamentary Assembly committee report, October 2001
4. 2015 National Military Strategy