How can technological and globalizing processes result in geopolitical and economic risks and how can we manage these risks/build resilience?

****

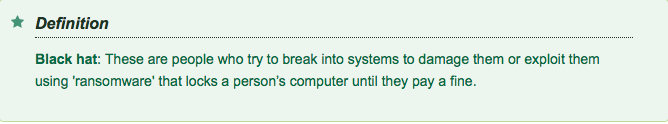
1. **Risks to individuals and businesses**

**Hacking**

* Hacking refers to the process in which individuals with knowledge of computer coding use software to help break into computer security systems.

**Threats to individuals, businesses posed by hacking:**

* Despite the benefits of computer technology, it has also made us vulnerable to **security hackers** who want to access information about us. Similarly, it has made governments who store huge amounts of information about us and our security vulnerable to threats from hackers.
* According to *Forbes*, during the US 2016 presidential election it became evident that Russian hackers had been able to get into the email of the Democratic National Committee, but they had also managed to get into the private emails of Hillary Clinton. It would appear that they had access to her private emails since 2013 and particularly her correspondence with her trusted adviser Sidney Blumenthal. This is an example of how an important individual can have their email account hacked.
* Hacking into people's private emails means that the hackers often have an insight into a person’s most intimate thoughts and transactions. Quite often the victims of such hacking are not in the public arena and are unaware that it has happened.
* There have been several instances in the USA and other developed countries of students or their parents hacking into the school records and altering grades to improve their chances of going to university. In the USA this is illegal and courts have punished people that have been caught doing this.
* In July 2015, a group calling itself "The Impact Team" stole the user data of Ashley Madison, a commercial website billed as enabling extramarital affairs. The group copied personal information about the site's user base and threatened to release users' names and personally identifying information if Ashley Madison would not immediately shut down. On 18 and 20 August, the group leaked more than 25 gigabytes of company data, including user details. Because of the site's policy of not deleting users' personal information – including real names, home addresses, search history and credit card transaction records – many users were publicly shamed. On 24 August 2015, Toronto police announced that two unconfirmed suicides had been linked to the data breach. Additionally, 1,200 Saudi Arabian email addresses were in the leaked database, in Saudi Arabia adultery can be punished with death.
* In May 2017 there was an attack by a cyber worm called WannaCry, on people using Microsoft Windows that effectively locked the computer and did not allow the users to access any of their material until they paid a ransom. It affected global users such as FedEx and Nissan, individual users and parts of Russia's Rail and Interior ministry, Britain's National Health Service, Deutsche Bahn (The German rail system) and Spain's Telefónica company. Overall it was said to have affected 75,000 computers in 99 different countries. This was an example of **black hat** hacking. Fortunately, a solution was found to deactivate the cyber worm. It appears that this virus came from North Korea.



**Threats of hacking to governments/states:**

United States  
**2007:** The US launched the Stuxnet worm against [Iran](https://www.wired.co.uk/topic/iran) to sabotage that country's nuclear program.  
**Outcome:** Stuxnet succeeded in briefly setting back the Iranian nuclear programme. The attack set a precedent for cyberwarfare: countries now launch digital assaults to resolve political disputes.

China  
**2014:** China breached several databases belonging to the US Office of Personnel Management.  
**Outcome:** The hackers stole sensitive data, including Social Security numbers, relating to more than 21 million people who had been interviewed for government background checks.

Israel  
**2014:** Israel allegedly hacked Russian security firm Kaspersky Lab to obtain intel on its research about nation-state attacks. It also struck venues in Europe where the UN Security Council met to negotiate Iran's nuclear programme.  
**Outcome:** The attackers may well have obtained intel about [Kaspersky](https://www.wired.co.uk/topic/kaspersky)'s research.

Israel  
**2012:** Suspected of launching the Wiper attack against the Iranian oil ministry and the National Iranian Oil Company.  
**Outcome:** The malware wiped hard-drive data, then erased system files, causing the machines to crash and preventing them from rebooting. Iran insisted it had data backups.

North Korea  
**2013:** Computers in South Korea were struck by a logic bomb that caused data deletion as well as preventing rebooting. South Korea blamed [North Korea](https://www.wired.co.uk/topic/north-korea) for the attack but it has never produced solid evidence.  
**Outcome:** Two broadcast-media companies and at least three banks were affected.

Russia  
**2014:** Russia allegedly hacked the US State Department and the White House.  
**Outcome:** The attackers had access to unclassified emails for President Obama as well as non-public details about his schedule.

Russia  
**2015:** TV5Monde, a French-language broadcaster, is hacked -- reportedly by Russia. A group calling itself the CyberCaliphate took credit, but French officials have pointed the finger at the Kremlin.  
**Outcome:** The hackers blacked out broadcasting for several hours and posted messages expressing support for ISIS to the TV channel's social-media accounts.

**Identity theft**

**Identity theft**: This is when a hacker steals another person's identity, generally online, to use for their own profit. It may involve the theft of bank and/or credit card details.

* Identity theft is becoming a growing international problem.
* Criminals have gained information about individuals from stolen or mislaid cards or they are able to hack the information from a person's email account.
* They then sell that information and it allows the recipient to apply for a credit card or adopt the person's identity to purchase goods.
* The international agency C6 Intelligence currently estimates that over 300,000 identities are being sold daily on the Dark Web.
* The major banks and credit card companies have tried to develop a number of ways to stop this. You may have experienced this with your own or that of your parent's credit card where the company sends a code to your mobile phone to authorise your online payment.
* However, identity theft has become one of the most significant consumer complaints.

**Surveillance**

Surveillance is monitoring the behavior of individuals and groups.

* There is a massive amount of surveillance of our financial transactions. Banks and finance companies sell information about their clients that help companies to target their marketing activities. There are more and more financial transactions, whether by credit card or phone, to purchase groceries, or to pay for a concert ticket, and each transaction reveals quite a lot about us as consumers.
* In towns and city centres our every move may be recorded on CCTV (closed-circuit television). Owners of businesses can keep a record of their customers and use this as a deterrent against theft and misuse of facilities. In most urban centres in high income countries you will find cameras recording the activities of citizens throughout the day and night. Police forces use these cameras as a means of checking the security of locations and businesses.
* On many major roads there are surveillance cameras to check the behaviour of motorists and to check congestion. Information can then be broadcast to other road and transport users.
* When you have your mobile phone turned on, the authorities know exactly where you are at any given time because your phone transmits your location information to satellites. There have, however, been proven societal advantages to this information being accessible. For example, monitoring of social media accounts prevented some potential terrorist attacks occurring in Belgium. The security services were able to raid and arrest a number of people who were planning bomb attacks.

### Government surveillance

* However, the most comprehensive surveillance of people's lives often comes from government agencies. Edward Snowden was a contracted analyst with the USA's National Security Agency (NSA) who was appalled by the amount of illegal information collected by the US intelligence agencies, the UK, Germany and others. This involved phone tapping and bugging of United Nations (UN) agencies, the Brazilian Energy Agency and ordinary citizens. In addition to that, emails and phone records of millions of ordinary citizens were being collected.
* Ben Emmerson, QC, who is the UN's main rapporteur on counter-terrorism believes that the mass surveillance carried out by the NSA and the UK's Government Communications Headquarters infringes individual rights and does little to reduce the threat of terrorism in either country. Moreover, it breaks international law, specifically Article 17 of the UN's International Covenant [agreement] on Civil and Political Rights. Article 17 of the covenant states that 'no one shall be subjected to arbitrary or unlawful interference with his [or her] privacy, family, home or correspondence, nor to unlawful attacks on his [or her] honour and reputation.

**Facial recognition technology e.g. China**

* A **facial recognition system** is a technology capable of identifying a person from a digital image or video frame from a video source.
* They work by comparing selected facial features from given image with faces within a database It is also described as a Biometric Artificial Intelligence based application that can uniquely identify a person by analysing patterns based on the person's facial textures and shape.
* Such technology has become very popular in China. Indeed, the Chinese start-up, Sense-Time, is a Chinese A.I. powered facial recognition system that is likely the most powerful in the world. This start-up has been named the most valuable startup in the world, with a valuable of $4.5 billion.

**Benefits of facial recognition in China:**

* Facial recognition can be used to speed up and improve the security of a multitude of transactions e.g. checking in at an airport or withdrawing money from an ATM.
* It may also be used to help track fugitives and missing people.

**However, facial recognition technology is open to criticism and abuse:**

* In China, the technology is used to publicly shame people, even for minor infractions such as jaywalking. Cameras will detect an individual and post their photo and offence to a billboard screen.
* The technology is also being used to discriminate against minorities in China. For example, there are over 11 million Uyghur people in Western China, these are ethnically Turkic Muslims who are discriminated against in Chinese society. Facial recognition technology is used to oppressively monitor Uyghurs and track their movements e.g. alerts are sent to the authorities when people stray more than 300 metres from their home.

**How can the risks posed by cyber-attacks and identity theft be managed by improvements in technology e.g. through increased cybersecurity and the use of e-passports?**

## **Cybersecurity in the USA**

The Department of Homeland Security in the USA has three different arms of its operations, which are dedicated to **defeating cybercrime and enhancing cybersecurity.**

### ****The US Secret Service****

* The US Secret Service maintains Electronic Crimes Task Forces, which aim to track down people who are trying to hack their way into banks and data banks.
* In cooperation with other governments and security services it has helped to track down criminals internationally who have stolen credit card details, defrauded banks and who have illegally entered data providers.
* It runs and organises the National Computer Forensics Institute to help train judges and police officers in understanding cybercrime.

### ****US Immigration and Customs Enforcement****

* One of the tasks of this group is to consider the issues of child exploitation and also of people smuggling and trafficking. It also runs a cyber forensics unit that looks at how to retrieve data from computers and systems.

### ****Law Enforcement Cyber Incident Reporting unit****

* This acts as a coordinator of information and provides advice to state and local governments in the USA about how to report cybercrimes.
* In the USA, the Department of Homeland Security provides a service to protect the security of the US government. It has created the [National Cybersecurity Protection System](https://www.dhs.gov/national-cybersecurity-protection-system-ncps) (NCPS), which provides intrusion detection, advanced analytics, information sharing and intrusion prevention capabilities that fight cyber threats to the Federal Executive Branch.
* It has created an early warning system called Einstein, which outlines the threats to US government systems from cyberattacks.
* The threats in cyberspace are, of course, global and the USA is working with government agencies in Australia, the UK, Canada and Israel as well as the European Union (EU).
* In May 2017 the USA agreed to a joint research venture with the Netherlands and in particular the [Netherlands Organisation for Scientific Research (NWO)](https://www.nwo.nl/en). Some research projects about how to improve cybersecurity that the group have worked on are:
* reducing the incidence of malware on smartphones
* developing models for cybersecurity protection for private firms
* improving responses to cyberattacks.

## **Banking cybersecurity**

* In 2014 there were just five cyber-attacks on UK banks that were reported to the Financial Conduct Authority in the UK; however, in 2016 there were at least 75 attacks.
* Andrew Davies, in an article in the International Banker, has argued for greater collaboration between banks and for increased data sharing to enable the banks to get to know their customers better to tackle fraud and money laundering. He argues that banks need to constantly renovate their systems.

## P**ersonal cybersecurity**

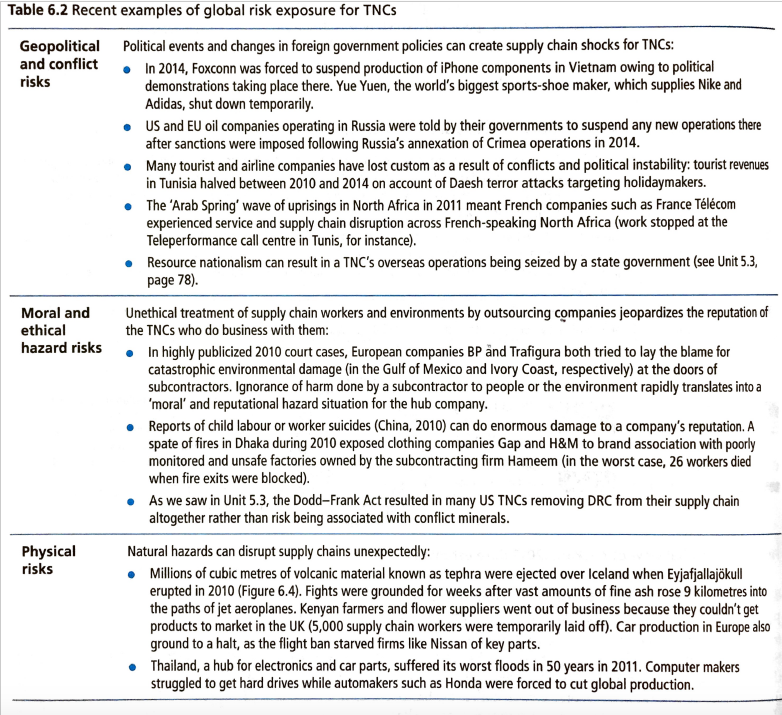
* It is important that you install antivirus software on your computer to tackle malware and adware. These forms of cyber-infection can often come via emails or by accessing a particular site.
* If you do banking online, make sure that the URL has https// at the beginning. The 's' at the end ensures that the transaction is secure.
* Be careful of emails that appear to be from your bank or government. They may be false and want you to share information with them.
* Know what your bank's official website looks like. Sometimes criminals deliberately change the appearance of the website to deceive you into giving information.
* Do not allow your computer to save logins and passwords as they can be acquired by malware and used to defraud your account

**E-passports**

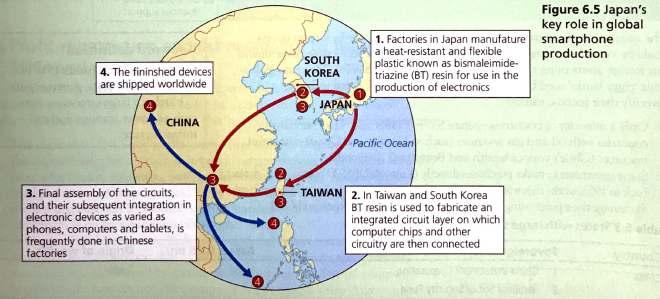
* **An E–passport**is a passport that contains a facial image as well as biometric data (such as fingerprints) about the individual. The data are stored on an electronic chip embedded in the passport. The authorities can only retrieve this data when a person enters a country.
* The USA wished to implement a more secure passport system after the 9/11 terrorist attacks of 2001. The Council of the EU issued a regulation in 2004 stating that all member states of the EU must have e-passports. In 2005, Germany became the first European country to introduce them, although Malaysia had introduced them as early as 1998.
* The e-passport contains biometric data, including fingerprint and iris information, making them much more difficult to forge and making it much more difficult to extract the data by skimming. This generation of passports requires the reader to authenticate itself with the chip inside the passport. The communication between the chip and the reader is encrypted, making the illegal taking of data difficult.
* The USA and Canada began sharing information about third country travelers in December 2012. The
* information included personal data about them. Both countries have online travel requirements that have to be filled in, which relate to the parental background, criminal records, drug usage and whether they have been involved with terrorist organisations. In addition, it includes information about the person's possible refugee status. There have been concerns about infringements of individual rights in both countries.
* Several countries have online visa systems that require you to stipulate which countries you have visited as an individual and your activities there. Russia, for example, requires you to mention which countries you have visited in the last 10 years. Exactly how much and what information is shared between countries is not clear, especially if you are required to give indications of financial status.
* After the European migrant crisis began in 2015, border controls within Europe have become stricter. For example, in 2016 Sweden implemented very strict controls of people coming from Denmark – before embarking on a train to Sweden from Copenhagen's airport it became necessary to show your passport so that they could ascertain that you were not a refugee.
* Switzerland, which is part of the Schengen Agreement (which allows movement between most EU countries without showing passports) has been much tighter in the last 2 years in checking travel documents at the border for all forms of transport.

1. **How can the supply chain flows of TNCs be disrupted by physical, economic and political processes?**

* A supply chains is the links between the producers of a good and the consumer that purchases it.
* The table below shows different types of risks posed to the supply chain flows of TNCs.



**How the Tohuku Earthquake/tsunami 2011 disrupted supply chain flows:**

****

**Japan’s Exposure to Risk**

* The 2011 natural disaster in Japan brought to light the fragile nature of the global supply chain.
* The event was the worst disaster to hit the country since World War II.
* Japan is an epicenter of high-tech manufacturing e.g. it plays a key role in the production of electronics such as smart phones (see above).
* In the aftermath of the 2011 disaster many manufacturers scrambled to replace suppliers disrupted.
* About 22 percent of the world's 300 mm silicon wafer supply came from the Shin-Etsu Handotai's Shirakawa plant in Fukushima prefecture, and 60 percent of critical auto parts were in the same area, The area is also a primary supplier of lithium battery chemicals, flash memory, and anisotropic conductive film used in LCD flat panel displays.
* In the race to provide better quality at lower prices, manufacturers picked very narrow, optimized supply chains.
* The disaster caused many companies to rethink their supply chain strategies, which suddenly seemed extremely fragile.

1. **Threats to the political and economic sovereignty of states**

**Tax avoidance and profit repatriation**

* Transnational corporations (TNCs) prefer to locate where they can minimise costs to themselves and maximise profits.
* Each country has different tax laws and also different rates of taxation.
* TNCs such as Apple, Google, Microsoft and Starbucks have offices in the USA where they pay company tax, but most of their wealth and cash may be in other countries that they operate in.
* These companies are able to reduce their tax in the USA and other higher tax countries by claiming losses from their subsidiaries (in lower tax countries) and leaving their money in those lower tax countries. This helps the company to minimise their tax obligations in countries such as the USA and the UK where the company taxes are higher.

****

**What is reshoring? How can political and economic risks be mitigated by reshoring?** Reshoring involves companies abandoning lengthy supply chains and instead returning productive operations to the country where it is headquartered**.**

* In an attempt to attract US companies to reshore, President Donald Trump wishes to cut corporate tax from 39.6% to 15%.
* He also wants to allow US companies not to be taxed on profits made overseas.
* This would be a great incentive for companies to return to the USA.

****

**How do wealthy individuals avoid paying tax?**

One way is to invest in schemes or projects that guarantee a tax relief for investment into them. In Ireland, people could get tax relief from investing in films on an individual basis up until the end of 2015. However, now that is being restricted to film producers.

Another way is to start a company yourself. In Switzerland, the Federal Council has agreed to incentives, grants and tax relief for start-up companies in a decision announced in June 2017. This is to encourage entrepreneurship. The start-up company can make a loss and this is a form of tax relief. At the same time the company can pay the individual a fee for their services.

**Start-up companies:**These are companies set up by entrepreneurs in ventures that are completely new.

A third way is through charity. In the USA, donations are tax-deductible, and there are various tax benefits for charities. Another way that has been used by wealthy individuals is to keep ownership of a property but to allow the charity to use the property without paying rent on it. At the end of a 10-year period it would be possible to take the property back and then sell it, making a large amount of money on the capital gain from the sale.

A further way to minimise tax is to invest money offshore in a shell company or in a bank account. Recently, documents released by an attorney's office in Panama highlighted some of these practices. The prime minister of Iceland had hidden some of his money in one of these companies and it was alleged that several of Putin's allies had money hidden from tax authorities there.

**Shell company:**This is set up by a firm of lawyers and is registered in a tax haven such as Panama. The lawyers are listed as the owners, but the company does not actually produce anything, it is just a place for people to hide their money from tax authorities at home.

A final way to minimise tax is to invest money in secret accounts offshore. Uli Hoeness, the president of Bayern Munich Football Club was caught by German tax authorities for putting millions of euros into Swiss bank accounts that he had hidden from them. He was fined and sent to prison for tax evasion when he was discovered.

## **Tax havens**

A **tax haven** is a country where companies and individuals pay little tax.

Tax havens can be hard to define and locate. However, the main feature of a tax haven is that its legal and financial setup can be used for minimising tax (through avoidance or evasion)... [compared with the tax that would be payable in other jurisdictions].

Until recently, secrecy was a major factor in that banks would not easily give up information on their holdings and legal entities to tax collectors. But now the [G20](http://www.g20.org/) is putting pressure on offshore tax havens to open up their doors and become more transparent in their dealings (or face sanctions), while at the same time granting tax 'amnesties' to encourage those with undeclared funds to come forward.

**Why should we care?**

If companies or individuals have their wealth stored in a tax haven rather than the country where most of their operations are based, it means that the operations-based country receives less money and may not have enough money to pay for social services such as pensions and health care or education. Portugal, Italy and Greece have all been severely affected by corporations and individuals avoiding paying tax in their country.

1. **Technological threats to states**

* **A disruptive technology is a technology that brings major changes to the way people live and work.**
* **We will look at drones and 3D printing as examples of disruptive technology.**

**Drone technology:**

Drones are robotic aircrafts that have brought about numerous changes in the way people live and work.

**Benefits and threats posed by drones**

1. **Surveillance and privacy infringements**

* Drones represent a threat to states in that they are being used to infringe people's personal rights and liberties.
* In Europe, media outlets have used them to fly over people's properties and take pictures of them at home.
* They have taken unauthorised photos of people sunbathing or enjoying the privacy of their garden. If they have facial recognition software, speakers and infrared technology, they could be particularly intrusive.
* If drones were interconnected, they could follow people over a large area.
* A concern is that drones could be miniaturised and be on a windowsill and go unnoticed.

1. **Drones are used to track crime -** In the USA a growing number of police departments are using drones to track crimes in their cities, The US Customs and Border Patrol also use drones to monitor the US-Mexico border to help them prevent illegal immigration.

**Benefits:**

* Drones can in used in place of helicopters, that are much more expensive.
* Drones can keep officers out of dangerous situations and cover more ground quickly -- say, in the case of a missing child or an armed suspect on the run, especially in rural areas.

**Threats:**

* Many of the US states who are beginning to employ the use of drones have not considered putting privacy laws relating to their use into place – this threatens civil liberties. The use of drones often stokes fears in populations that government agencies intend to use them to spy on private lives.
* There potentials for abuses if police use these stealthy machines to run around warrant requirements.

1. **Drones are used by the military** - to gather intelligence information and to carry out airstrikes on targets e.g. they have been used by the US Air Force and the UK's Royal Air Force to carry out attacks on militants in Pakistan, Syria and Afghanistan.

**The use of drone technology is beneficial for the military because:**

* It provides surveillance and intelligence gathering activities in areas that would be hostile for normal aircraft.
* They can be used to listen to mobile telephone conversations, and to locate roadside bombs or devices on landing sites.
* They provide surveillance on local groups to see what the normal behaviour of the group is.

**Threats:**

* However, drone strikes are controversial as there is much debate about the legality of drone warfare under international law.
* There have been concerns about the collateral damage, with many more innocent people being killed than just the intended targets. Some estimate that 80–90% of the victims are innocent civilians. One such strike in the remote region of North Waziristan in Pakistan killed 40 people – mostly civilians – in March 2011. It is believed that most of these people were people attending a tribal meeting. In an attack in December 2013 in Yemen, a wedding party who were driving to the feast in cars were attacked by four Hellfire missiles delivered from US drones, killing 12 people.

1. **Use of drones by TNCs to deliver goods** – for example Amazon is expecting to be able to start delivering goods by drone in the near future.

**Benefits of delivery drones:**

* They save time as it will be quicker to transport goods to their destination – Amazon believe they would be able to achieve delivery of many goods (weighing under 5 Ibs) within 30 minutes.

**Threats of delivery drones:**

* **Privacy Breach:** Delivery drones use cameras while delivering the materials to target markets or locations. The cameras constantly record the actual location, property, and the person without their consent while receiving the object. Corrupt drone users may exploit recorded information of their consumers.
* **Easily Stolen:** Drones are suspended independently into the atmosphere. Anyone can take the drone away while disconnecting its power supply. Once stolen, companies will no longer have the authority to control their properties.

**Some further benefits of drones:**

* It is important to retain a balanced view about the use of drones because they can provide many benefits as well as threats. Unicef is working with Rwanda and Malawi to help deliver needed medicines to remote regions. They have found that by using drones they can cut the delivery time of drugs to minutes instead of hours or days.
* There is no doubt that drones will be of great use in remote areas in helping to reach people who have got into trouble. They can be used to find people in a much shorter period of time. There is also no doubt that drones can be used to improve the quality of maps and help, for example, geologists to identify potential sources of minerals.

**3D Printing**

**3D printers:**These devices let people print three-dimensional objects such as phone cases, jewellery, board game pieces and even tools

* Technological advances in 3D printing have been enormous in the last few years.
* Adidas has produced its blade soles with a 3D printer thus disposing with traditional manufacturing methods.
* The aeroplane manufacturer, Airbus, experimented with 3D airframes cut from their aluminium alloy, which are both lighter and harder than traditional methods. T
* These printers can also be used to manufacture medical instruments and also new hips for hip replacements.
* 3D printers thus have the ability to revolutionise life. They will enable us to print designs at home and also to enhance them. Why should they then provide a threat to countries and companies?

**Some relevant key terms:**

****

**Risks of 3D printing:**

**There are a number of issues about their use that will need to be considered that relate to intellectual property rights:**

* Breaching copyright with a 3D printer is relatively easy to do and as the printers come down in price many people will have the ability to copy designs or material at home. This will mean that like downloaded music and movies at home now, it will be virtually impossible to detect copyright infringements.
* In most countries the inventor owns a patented invention for a lifetime (20 years in Germany). There are a number of items that are patented, such as prostheses and hearing aids, that it will be possible to make at home as they have a fairly simple design. It will be possible to make these items without infringing patents. It is only if they are going to be sold that it will become a problem.
* Trademarks of copied items are similar to patents in that there will only be issues of falsely using the trademark if items are sold.
* Many goods are currently produced where copyright, patents or trade secrets have been ignored. This has cost companies and countries a great deal of money. China has taken some time to recognise intellectual property rights in all spheres, although its record has improved since 2011. They are stepping up their investment in the development of 3D printers and are aiming to become the design capital of the world.
* It was estimated that the sale of 3D printers would be greater in China in 2016 than in the USA. The Chinese government, who are anxious to reduce production costs and to enhance current designs of materials, is supporting this. The Kangshuo Group has received a grant of US$15 million to have a 3D printing centre.

**There are other risks with 3D printers:**

**For example:**

* 3D printing has important implications for state sovereignty and the ability of governments to control what can pass across state borders. I.e. it is easier for a state to intercept an illegal shipment of guns than the blueprint to be emailed to a 3D printer.
* This creates a technological disruption- physical commodity movements are being replaced with information exchanges which are harder to control.

1. **The correlation between increased globalization and renewed nationalism/tribalism**
2. Define the terms nationalism and tribalisation
3. Outline two case studies to show increased geopolitical tension/conflict i.e. increased nationalism in the United States under Donald Trump and Brexit, UK.

**I WILL ADD NOTES ON THIS LATER – SUCH IDEAS HAVE PREVIOUSLY BEEN COVERED IN OTHER UNITS**

**Example exam questions**

* “Power struggles between places present the greatest threat to the ‘normal lives’ of individuals and businesses.” Discuss this statement. [16]
* Evaluate the threat posed to the political and economic sovereignty of states by profit repatriation and tax avoidance by TNCs. [12]
* Using examples, analyse how technological developments can threaten the security of states. (12)
* Examine the extent to which globalisation is responsible for increasing nationalism. [16]
* Globalisation is now in retreat because of the risks it has created. Discuss this statement (16)
* Evaluate the success of strategies used to manage the negative impacts of globalisation on people and places. (16)