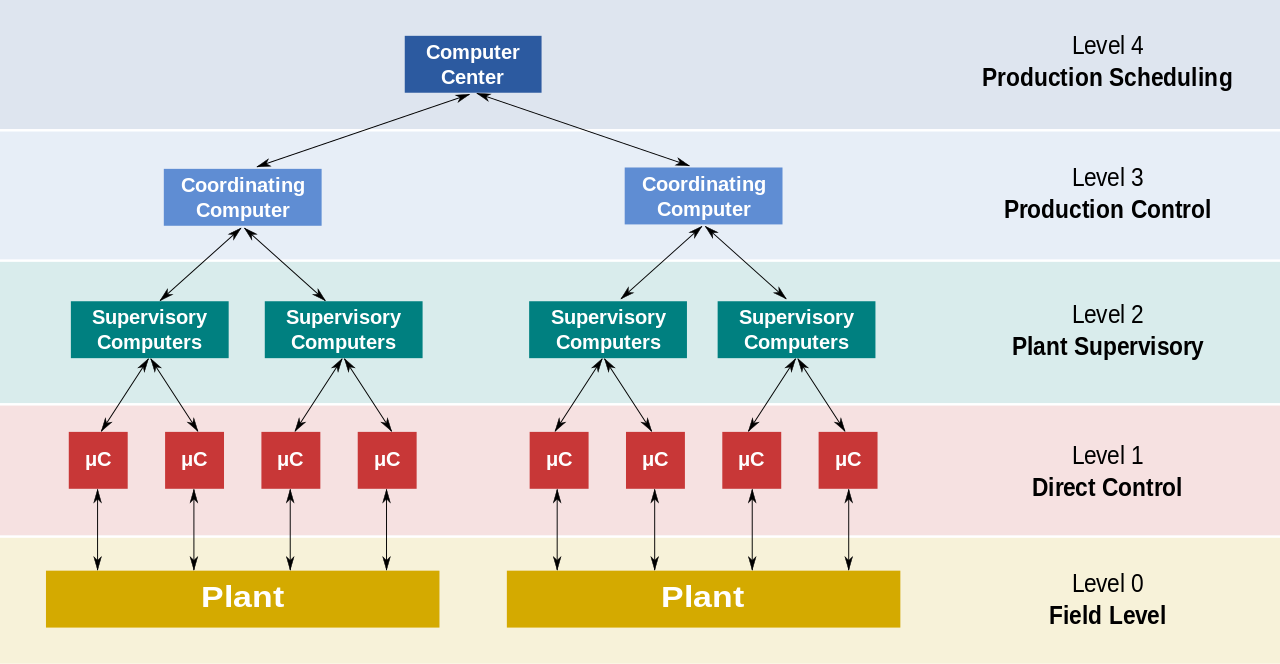
* A nation state is a type of state that joins the political entity of a state to the cultural entity of a nation, from which it aims to derive its political legitimacy to rule and potentially its status as a sovereign state.A state is specifically a political and geopolitical entity, whilst a nation is a cultural and ethnic one. The term "nation state" implies that the two coincide, in that a state has chosen to adopt and endorse a specific cultural group as associated with it.
* The concept of a nation state can be compared and contrasted with that of the multinational state, city state, empire, confederation, and other state formations with which it may overlap. The key distinction is the identification of a people with a polity in the "nation state."
* Non-state actors (NSA) are entities that participate or act in international relations. They are organizations with sufficient power to influence and cause a change even though they do not belong to any established institution of a state.
* Violent non-state actors (VNSA), also known as armed non-state actors, are non-state actors, i.e. "individuals or organizations that have economic, political or social power and are able to influence at a national and sometimes international level but do not belong to or ally themselves to any particular country or state,"[1] who employ violence in pursuit of their objectives. The term has been used in several papers published by the U.S. military. There are many reasons why violent non-state actors develop.
* Acronym for supervisory control and data acquisition, a computer system for gathering and analyzing real time data. SCADA systems are used to monitor and control a plant or equipment in industries such as telecommunications, water and waste control, energy, oil and gas refining and transportation. Functional levels of a manufacturing control operation



* SCADA Systems are widely used in the following:
  + Oil and Gas
  + Pipeline monitoring and control
  + Remote monitoring and control of production, pumping, and storage locations
  + Offshore platforms and onshore wells
  + Refineries, petro-chemical stations
  + Water and Wastewater
  + Water treatment centers and distribution
  + Wastewater collection and treatment facilities
  + Utilities
  + Electrical power distribution from gas-fired, coal, nuclear
  + Electrical power transmission and distribution
  + Agriculture / Irrigation
  + Manufacturing
  + Food and Beverage
  + Pharmaceutical
  + Telecommunications
  + Transportation
  + And many others
* Stuxnet is a [malicious](https://en.wikipedia.org/wiki/Malware) [computer worm](https://en.wikipedia.org/wiki/Computer_worm), first identified in 2010, that targets industrial computer systems and was responsible for causing substantial damage to [Iran's nuclear program](https://en.wikipedia.org/wiki/Iran%27s_nuclear_program). The software was designed to erase itself in 2012 thus limiting the scope of its effects. The worm is believed by many experts to be a jointly built [American](https://en.wikipedia.org/wiki/US)-[Israeli](https://en.wikipedia.org/wiki/Israel) [cyber weapon](https://en.wikipedia.org/wiki/Cyberweapon), although no organization or state has officially admitted responsibility. Anonymous American officials speaking to [The Washington Post](https://en.wikipedia.org/wiki/The_Washington_Post) claimed the worm was developed during the [Bush administration](https://en.wikipedia.org/wiki/Presidency_of_George_W._Bush) to sabotage Iran's nuclear program with what would seem like a long series of unfortunate accidents.
* **Duqu** is a collection of computer malware discovered on 1 September 2011, thought to be related to the Stuxnet worm. The Laboratory of Cryptography and System Security (CrySyS Lab) of the Budapest University of Technology and Economics in Hungary discovered the threat, analysed the malware, and wrote a 60-page report naming the threat Duqu.[3] Duqu got its name from the prefix "~DQ" it gives to the names of files it creates.
* The term **Duqu** is used in a variety of ways:
* ***Duqu*** malware is a variety of software components that together provide services to the attackers. Currently this includes information stealing capabilities and in the background, kernel drivers and injection tools. Part of this malware is written in unknown high-level programming language, dubbed "Duqu framework". It is not C++, Python, Ada, Lua and many other checked languages. However, recent evidence suggests that Duqu may have been written in C with a custom object oriented framework and compiled in Microsoft Visual Studio 2008.
* **Duqu** flaw is the flaw in Microsoft Windows that is used in malicious files to execute malware components of Duqu. Currently one flaw is known, a TrueType-font related problem in win32k.sys.
* Operation Duqu is the process of only using Duqu for unknown goals. The operation might be related to Operation Stuxnet.
* **Flame**,[a] also known as **Flamer**, **sKyWIper**,[b] and **Skywiper**,[ is modular computer malware discovered in 2012that attacks computers running the Microsoft Windows operating system.The program is being used for targeted cyber espionage in Middle Eastern countries.
* Its discovery was announced on 28 May 2012 by MAHER Center of Iranian National Computer Emergency Response Team (CERT), Kaspersky Lab and CrySyS Lab of the Budapest University of Technology and Economics. The last of these stated in its report that Flame "is certainly the most sophisticated malware we encountered during our practice; arguably, it is the most complex malware ever found." Flame can spread to other systems over a local network (LAN) or via USB stick. It can record audio, screenshots, keyboard activity and network traffic. The program also records Skype conversations and can turn infected computers into Bluetooth beacons which attempt to download contact information from nearby Bluetooth-enabled devices. This data, along with locally stored documents, is sent on to one of several command and control servers that are scattered around the world. The program then awaits further instructions from these servers.
* Kaspersky Lab researchers have discovered a “complex cyber-espionage toolkit” called **Gauss** which is a nation-state sponsored malware attack “closely related to Flame and Stuxnet,” but blends nation-state cyber-surveillance with an online banking Trojan. It can steal “access credentials for various online banking systems and payment methods” and “various kinds of data from infected Windows machines” such as “specifics of network interfaces, computer’s drives and even information about BIOS.” It can steal browser history, social network and instant messaging info and passwords, and searches for and intercepts cookies from PayPal, Citibank, MasterCard, American Express, Visa, eBay, Gmail, Hotmail, Yahoo, Facebook, Amazon and some other Middle Eastern banks. Additionally Gauss “includes an unknown, encrypted payload which is activated on certain specific system configurations.

Assignment. Submit in 8.5x11” paper, stapled font Arial 11 pts 1.15 spacing. Expected outputs: There will be no limit on words, but with the expected number of questions, about 5 pages will do.

1. What is your reaction on the presentation regarding cyberwars? Cite your own opinion with facts on how cyberwar, cybercrimes and/or cyberterrorism, thrive today.
2. With regards to the European Convention on Cybercrime, was their conclusion substantial enough to assure and educate the IT industries, government, and the public regarding these threats?
3. List about 5 examples of cyber malwares, determine the origin, how was it spread and the effects.