NUMBER	TOPIC	EXAMPLES
1.	**Challenges of engineers**	
1.1.	Autonomous sensors for mine detection	
1.2.	Transportation of explosives (ex. with drones)	1.2.1. Suicide drones (some can carry explosives, some carry other cargo, that makes enemy troops out of alignment (ex. liquid) It can be swarm of drones.
1.3.	Initiation of blasting (freely available resources)	1.3.1. Compact blast initiator. Blasting machine should be lightweight, safe, shock and water-resistant, cheap (disposable). Must operate with 500 m wires and 5 el. detonator. 1.3.2. Mobile explosive change remote control.
1.4.	Interactive map (route drawing, APP-6 (C) signs, etc.)	1.4.1. App for the communication in real-time can show you (or imitate) the contamination; 1.4.2. App for the adjusting photos, where you can add a tactical sigs etc. 1.4.3. App for landscape scanning where is included graphics system.
2.	**Challenges of cyber security**	
2.1.	Open source analysis, aggregation of public data, parsing tool	Open source, pastebin analysis, aggregation of public data, parsing and threat intel. Open Source Analysis supports cyber threat intelligence and identification. The information is used by the organization to understand and anticipate current and emerging threats against the organization. This information is used to prepare for protection, prevention, and identification of cyber threats that could cause harm. Malware authors, for example, often store part of the malicious content in their malware on it, and then fetch it later from inside the malicious executable using the share link. Pastebin data can store anything from Credentials and Sensitive Information, cryptocurrency keys and wallets to other sensitive information.
2.2.	Content Management Systems (CMS) vulnerability assessment	Content Management Systems (CMS) vulnerability assessment. An adversary uses automated tools to scan the internet for security vulnerabilities to exploit in order to gain access to a web server. Once a CMS has been compromised, an adversary can exploit their access to obtain access to authenticated and privileged areas of a web application; upload malware to the web server to facilitate remote access, inject malicious content into legitimate webpages
2.3.	Optimization of the CERTs‘ Incident Management Process	Organizations of all sizes and types plan cyber security incident management process. A typical incident response plan includes six phases which help the affected organization recover from an attack or simply contain it once it occurs – preparation, identification, containment, eradication, recovery, and lessons learned. Automating organization’s response to security threats enables security operations team to triage alarms more effectively, respond to critical events faster, and seamlessly integrate existing security solutions into a more efficient and comprehensive incident response program.

3.	**Alternative communication channels/ways**	
3.1.	Alternative communication channels/ways	3.1.1. Hard to find radio communication - example hiding at the frequencies used, to avoid disruption to basic communication channel; 3.1.2. Laser communication in various locations, using different kind of platforms (eg.: towers, tall buildings, drones) 3.1.3. Portable tactical level antennas/ system for triangulation and communication location; 3.1.4. Mobile directional antenna (portable, lightweight)
3.2.	Radio stations from freely available resources	3.2.1. Radio stations made from different communication equipment, eg. phones, walkie talkie radio stations, etc. need for high-frequency radio stations up to 5-10 W, 3-8 Mhz. and very high, ultra-high frequency with the ability to control frequencies in a wider range than the civilian market. 3.2.2. Opportunities for upgrading existing obsolete electronic media; 3.2.3. Radio amplifier (portable, for signal amplification)
3.3.	Alternative encryption and decryption devices	3.3.1. Alternative encryption options: non-specific algorithms utilization 3.3.2. Development of software which can calculate and evaluate communication capabilities of different radio communication systems (LAD, UAD, AD) according to input parameters (radio station, antenna type, frequency, encryption) and terrain characteristics (terrain, vegetation, cities, power lines) 3.3.3. A platform/ an app that can be used to set up LAD/ UAD (VHF/ UHF) waves visibility (LOS)
3.4.	Communication jammer from freely available resources	3.4.1. GSM/GPS communication jammer 3.4.2. Radio attenuation system (EW) flying/ ground
4.	**Bottom up**	