NOTE

Retamares, Madrid

Safer Internet Day (SID) - cyberspace vulnerabilities, cyberwar and digital threats

- FEB 7TH is Safer Internet Day and we take the opportunity to take a look at the current landscape and understand more about cyber-threats

07. FEB. 23. Today our country faces numerous threats. The historical national security perspective, marked by conventional risks and terrorism, must be broadened to include more and more vulnerabilities. On today's Safer Internet Day, it is appropriate to review the risks brought about by digitisation and the hybrid nature of any attack we may receive, especially cyber threats that come with the use of the internet.

Since 2007, NATO has considered the hybrid nature of conflicts as one of its top priorities, and Spain, as a member of this organisation, echoes the implications of this. Disinformation, individual-level terrorism, fraud, increasingly aggressive espionage and, of course, cyber-attacks are just some of the threats that make up hybrid conflict. Moreover, expanding digitisation exacerbates the latter risk, and awareness is one of our main tools to mitigate both the effect and the chances of the enemy succeeding when carrying out such digital attacks.

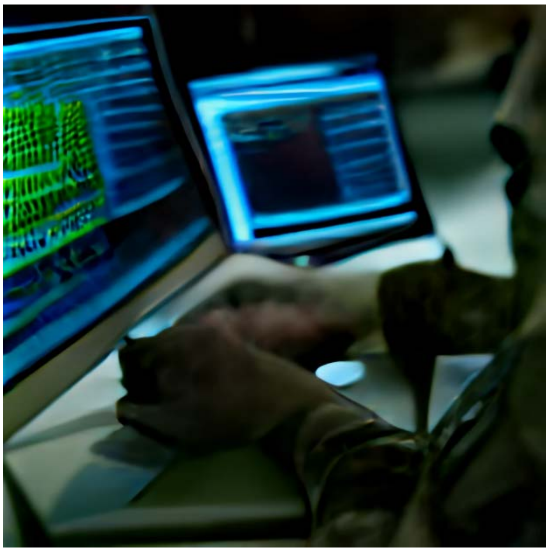
In 2010, Richard A. Clarke warned the US administration of one of the most pressing risks it would face in this century, defining cyberwarfare as "any unauthorised penetration by, on behalf of, or in support of, a government of computer equipment and networks, where the purpose is to add to, alter, falsify, steal, or damage the information, functioning or operation of such equipment. It is therefore easy to understand that cyberwarfare involves conflict situations characterised by deliberate attacks and should be considered as such, given the critical nature of today's cyber-based systems and infrastructure, or those that rely on digital systems and networks.

While these threats translate into actual attacks that are executed on a daily basis, it is worth considering that the breadth of their reach is not limited to targets that are military powers, but many other civilian, public and private targets such as power grids, the financial system and even supply chains are also threatened. Recall the effect that the COVID 19 pandemic had on this last element of our present day and you can imagine the huge impact that a series of successful cyber-attacks would have on the internationalised and interdependent supply chain. The irrelevance of the effect of geography and the ease of the cyber environment for surprise attacks further increase our country's need for security.

Cyber-attacks are most effective against adversaries who are least prepared to defend themselves and, in this sense, a technologically developed country such as Spain becomes a profitable target the less able it is to defend itself against a sophisticated and persistent attack. It is not only our cybersecurity institutions, with the MCCE (Spain’s Joint Cyberspace Command) at the forefront, that are the essential elements to guarantee this security since, on this occasion, each and every one of us individually is responsible and an active member in protecting Spain. At the keyboard, we are all "soldiers" or "victims". Today, of all days of the year, let us keep our digital footprint and our online presence safe and celebrate SID in defence of our country.

Protect yourself, protect your family and you will protect the Armed Forces

Cyber threats: the latent risk



Constant vigilance is the best asset