INTERNET AS A METHOD OF TROLLING OFFENSIVE INTELLIGENCE OPERATIONS IN CYBERSPACE

Dragan Djurdjevic
Academy of National Security, Belgrade
Miroslav Stevanovic Security Information Agency, Belgrade

Abstract: The paper analyzes Internet trolling as an operational intelligence activity, and the challanges it presents for national security, as well as the assessment of possible strategic protection of national cyberspace. This problem arises since collecting the data through automated programs eliminates guarantees of ethical grounds for their gathering in terms of clear reason, integrity of motives, proportionality of methods and the relevant authority. The basic thesis is that intelligence gathering on the Internet may be used against the basic values of states. Functionally, due to characteristics of the targets, trolling is conducive for collecting strategic information related to individual and collective attitudes and their contextualization; or the economic entities and critical infrastructure of national crisis management system, as well as for the influence on the political decisions. Also, because of the network properties, it is suitable for identifying, locating of potential sources of information and gaining their cooperation on the basis of motivation to support the objectives. The tasks of cyber data collection include psychological profiling, imposing attitudes, conducting secret surveillance on a massive scale and interception of communications. Internet trolling enables an access to primary data on the territory of other states, and thus it is suitable for secret and covert "installation" in the online community; for organized attack to infiltrate the government systems; for military and political interests; and for sabotaging various national infrastructure, communication and other systems. Structurally, the use of trolling as a mean of collecting data stems from the military development, today applied within the doctrine of "Full Dimension Operations". It is conducted in an organized manner, with legend and rules of secrecy, so the trolls are agents of authorised agencies. Intelligence systems, like the "Five Eyes" (FVEY - the USA, GB, Australia, Canada and New Zealand) have software tools, available IP addresses and networks of computers which run programs difficult to identify (botnet), which allows them to troll undetectedly. The methods and tasks revealed through structural and functional analysis enable the induction of threats and challenges for national security of other states. The principal challenges are the consequence of automatized methods and are democratic in nature. The primary risk for national security is the fact that it involves secret and organized efforts by other states to influence public opinion and dehumanization. Another is due to the fact that agencies of some countries have a capacity to secretly monitor communications in the cyberspace of other countries. Intelligence trolling can have an online operation against a certain state as an immediate goal, like misinformation and disinformation, creating HUMINT networks, or cyber attacks on critical infrastructure. With an aim to master the Internet, the FVEY agencies are trying to invade every possible system on the global net, searching to gain access to further systems. The strategic protection of national security in cyberspace requires a multi-dimensional approach, within the framework of the national security strategy. It must include science and research of the cyber space and social networks, as the preconditions; education for the use of the Internet at all levels, quality education and public information systems, in sense of prevention; and the criminalization of fraudulent messages and training of the judiciary for prosecution, in terms of repression.

Keywords: Internet trolling, secret Internet operations, mastering the Internet, online targets, Internet sabotage, full-spectrum operations.

Pages 13-32