DON'T JUDGE INSURGENTS BY THE CLOTHES THEY WEAR

Major Dennis Zijp

The AJP-3.4.4 Counterinsurgency[1] is a thematic doctrinal NATO publication for the operational commander that conducts operations within a security campaign as part of a counterinsurgency[2]. The first version of this publication will be reviewed and rewritten in the next two years. One of the lessons identified by NATO forces after more than a decade of experiences obtained in, among other locations, Iraq and Afghanistan is the change in modi operandi by the insurgents[3]. One of these modi operandi is the use of cyber space[4].

ABOUT THE AUTHOR

Major Dennis Zijp is staff officer C2 & C2 Support Systems Junior at the Land Warfare Centre in Amersfoort. Major Zijp is also the secretary of the NATO working group developing the doctrine publications AJP-3.4.4 Counterinsurgency and ATP-3.4.4.1 Tactical Activities in Counterinsurgency.

GENERAL

Insurgents, although frequently portrayed as poor and uneducated, prove to be very resourceful, intelligent and capable of developing and adopting capabilities to obtain their goals. One of these capabilities is the use of cyber space.

With the reduction in costs of ICT infrastructure and end-user equipment, expansion of the physical, logical and social network on a global scale and the tremendous possibilities of cyber space, almost everybody in the world can connect to cyber space and use it to some extend. Insurgents are known to use cyber space to conduct a full spectrum of cyber conflict, cyber mobilisation, command and control and psychological operations.

PROBLEM

The main problem concerning cyber in current operations is that operational and tactical commanders aren't fully situational aware of the impact the insurgents use of cyber space can have on their operations and tactical activities within a security campaign.

This results in not getting the advantage over the insurgents and an increase of having an opinion after the facts.

In order to become situational aware the operational and tactical commanders have to know what they are dealing with. What are the cyber capabilities insurgents are using?

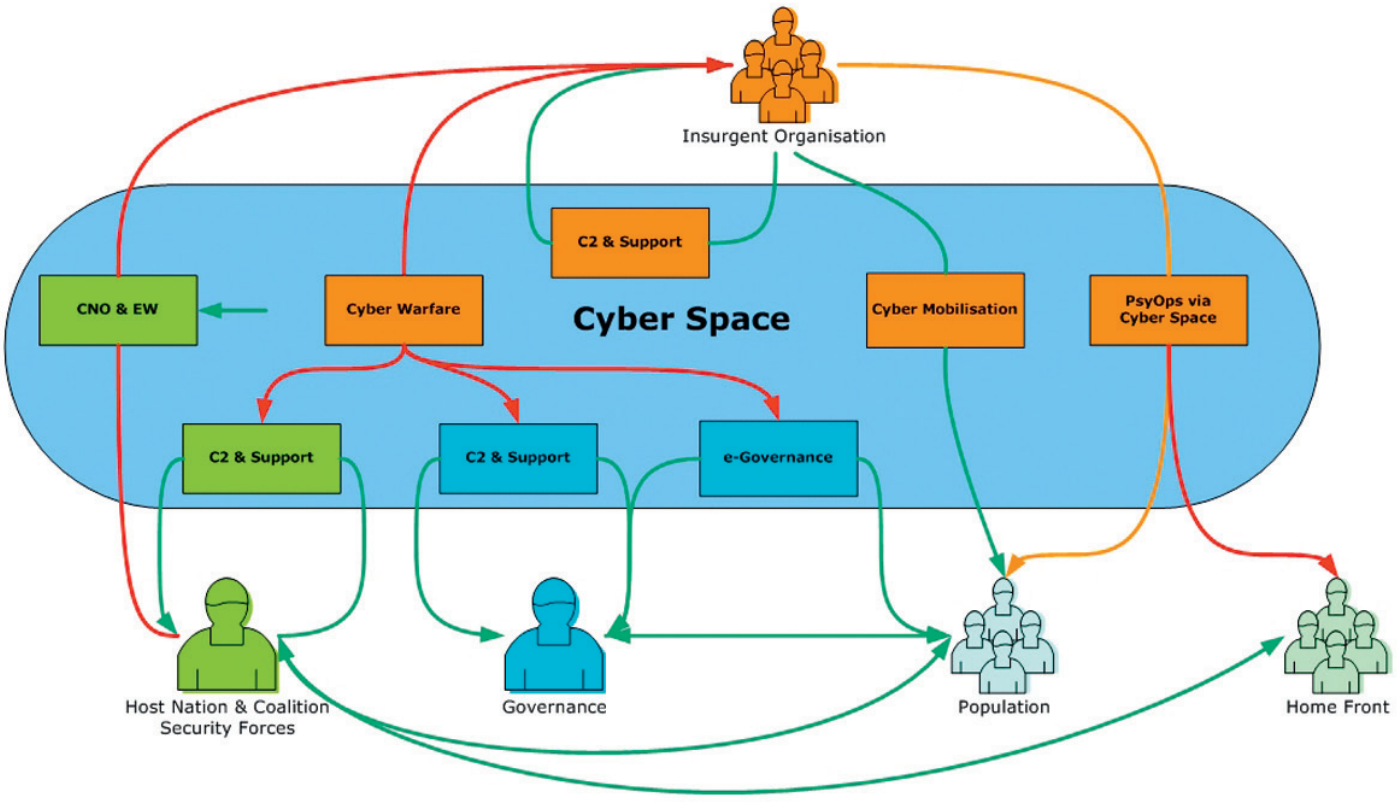

Figure 1: Cyber in counterinsurgency

FULL SPECTRUM OF CYBER CONFLICT

Insurgents can use the full spectrum of cyber conflict to attack governance and security forces, especially when the governance is evolving by implementing for example electronic-Governance (e-Governance) to improve communication and information exchange with the population and the economic sector. Cyber attacks are also possible on coalition forces to disrupt or deny continuation of the decision making process. Also cyber crime for example to obtain finances, cyber espionage to obtain critical information and cyber terrorism to create fear can be conducted by insurgents.

CYBER MOBILISATION

Insurgent organisations can use cyber mobilisation to recruit new insurgents and inform or activate followers from all over the world. This mechanism can create flows of new insurgents or followers from different (surrounding) areas to the theatre. In combination with the scoped situational awareness of the operational and tactical commander this can create an increasingly volatile situation.

COMMAND AND CONTROL

Insurgent organisations can use cyber space to command and control their activities. With cyberspace a large group of insurgents can be reached who are possible dispersed over a large area and even across borders. Issuing orders, exchanging knowledge and information, providing education and training guidance and even arranging finances and logistics for insurgent activities are handled via cyber space.

PSYCHOLOGICAL OPERATIONS

Psychological operations via cyber space can be used by insurgents to diminish the coalition home front support to the mission. This may even result in a growing aversion against the mission of the counterinsurgency coalition and can create political turbulence in the troop contributing nations. Also via cyber space influencing the local population is possible, by coercing not to cooperate with security forces and local or national governance while not opposing the insurgent's plan.
All four insurgent's cyber capabilities and their effects are illustrated, as an example, in figure 1 Cyber in counterinsurgency. In figure 1 the red arrows are representing the negative effect on the entities activity, the green arrows the positive effects and the orange arrows a mixed effect.

COMPUTER NETWORK OPERATIONS AND ELECTRONIC WARFARE

Now that the operational and tactical commanders know what they are dealing with, what's next? Operational and tactical commanders should consider creating a proactive mindset towards reducing the effects of insurgents' cyber capabilities on security forces, governance, population and home front.

Besides the use of the more traditional capabilities, a combined use of Computer Network Attacks, Computer Network Defence, Computer Network Exploitation and Electronic Warfare on a strategic, operational and tactical level can obtain information about, monitor of, disrupt or even deny the use of cyber space by insurgents. Thereby communication and information exchange between security forces, governance, population and home front will be at least maintained if not improved.

ALL IN ORDER TO WIN THE 'BATTLE OF PERCEPTION' AND TO KEEP THE 'FORCE PROTECTED'.[5]

[1] The Netherlands (Land Warfare Centre, department Land Warfare) is custodian of both documents.

[2] Counterinsurgency is the set of political, economic, social, military, law enforcement, civil and psychological activities with the aim to defeat insurgency and address any core grievances (AJP-3.4.4).

[3] Insurgency is the actions of an organised, often ideologically motivated, group or movement that seeks to effect or prevent political change of a governing authority within a region, focused on persuading or coercing the population through the use of violence and subversion (AJP-3.4.4).

[4] NATO Cooperative Cyber Defence Centre of Excellence (Tallinn, Estonia) is still working on a definition of cyberspace. For this article the definition of cyber space is: all entities that are or may potentially be connected digitally. The domain includes permanent connections as well as temporary or local connections and in all cases relates in some way to the data (source code, information, etc.) present in this domain (Royal Netherlands Ministry of Defence, The Defence Cyber Strategy, 2012).

[5] AJP-3.4.4 Counterinsurgency

REFERENCE LIST

The following articles and documents have been used:

NATO LOWG AJP-3.4.4 working group, Allied joint doctrine for counterinsurgency (COIN), version 1, February 2011

NATO LOWG ATP-3.4.4.1 working group, Guidance for the application of tactical military activities in counterinsurgency, ratification draft, June 2013

Timothy L. Thomas, Cyber mobilization: the neglected aspect of information operations and counterinsurgency doctrine, 2007, ATDC Fort Leavenworth USA

Samual Liles, Cyber Warfare: as a form of low-intensity conflict and insurgency, 2010, CCDCOE Tallinn EST

David W. Pendal et al, Cyberspace Operations in support of counterinsurgency operations, Land Warfare paper no. 95, April 2013, The institute of Land Warfare USA

Audrey Jurth Cronin, Cyber-Mobilization: the new levée en masse, 2006

TRADOC, Cyberspace operations concept capability plan 2016-2028, Pamphlet 525-7-8, 22 February 2010, United States Army USA

David Kilcullen, Counter-insurgency redux, Survival vol. 48 no. 4, Winter 2006-07, USA

Minister of Defence, The Defence cyber strategy, 27 June 2012, Netherlands Ministry of Defence The Hague NLD

Rain Ottis and Peeter Lorents, Cyberspace: definitions and Implications, CCDCOE Tallinn EST

Shailendra C. Jain Palvia and Sushil S. Sharma, E-government and E-Governance: definitions/ domain framework and status around the world, Long Island University Brookville New York USA

Samual Liles et al, Applying traditional military principles to cyber warfare, 2012, CCDCOE Tallinn EST