A finales del pasado mes de abril, el secretario de Defensa estadounidense, Ashton Carter, presentó la nueva Estrategia de Ciberseguridad del Pentágono. Titulado *The DoD Cyber Strategy,*este documento, que reemplaza a la estrategia de 2011, traza el camino a seguir y los objetivos a lograr en materia cibernética por el Departamento de Defensa (DoD) durante el periodo 2015-2018. Este es el primer documento de estas características que plantea abiertamente que Washington podrá realizar actividades de ciberguerra al afirmar que el país "debe ser capaz de recurrir a las ciberoperaciones para destruir las redes de mando y control, infraestructuras críticas o sistemas de armas de los potenciales adversarios del país".

También recuerda que las ciberoperaciones se integrarán plenamente en el planeamiento y conducción de las operaciones militares. Para ello, además de potenciar la constitución de cibercapacidades conjuntamente, el Pentágono ha planificado crear una ciberfuerza compuesta por 6.200 personas repartidas en 133 equipos cuyos cometidos principales están relacionados con la defensa, la inteligencia y el ataque en el ciberespacio. Además, el DoD ha comprendido que la formación y el plan de carrera de sus ciberguerreros son inadecuados. Por ello, el Pentágono tiene previsto desarrollar programas de intercambio con el sector privado, que disponen de planes de formación más avanzados y adecuados.

Washington ha planificado crear una ciberfuerza compuesta por 6.200 personas repartidas en 133 equipos.

Paradójicamente, aunque esta estrategia proporciona algunas ideas sobre cómo se podrá utilizar el elemento cibernético en las operaciones militares conjuntas, plantea abiertamente que EE UU podrá utilizar las cibercapacidades de manera ofensiva (y no solo en labores de ciberdefensa o explotación tras un ciberataque). Además, empieza a explicitar la doctrina de disuasión y trata la necesidad de incrementar la cooperación en materia de ciberseguridad entre las distintas Administraciones del país, entre los actores públicos y privados y entre los socios y aliados clave.

Este último aspecto es muy importante, ya que nos permite descubrir quiénes son los aliados de Washington. Por un lado, los socios del Five Eyes (Canadá, Gran Bretaña, Australia y Nueva Zelanda), seguidos por algunos países de Oriente Próximo y Asia-Pacífico (que serán empleados para apoyar la Tercera Estrategia de Compensación en materia de defensa) y algunos miembros de la Alianza Atlántica. En otras palabras, la OTAN, como organización, no es considerada un actor en la materia —hay que recordar que las cibercapacidades de la Alianza Atlántica cubren las necesidades operativas del cuartel general, estructura de mandos y organismos asociados, estando a disposición de sus naciones miembros en caso de necesidad— debido a las grandes carencias que tienen algunos de sus miembros y que comprometen la capacidad de actuación de la Alianza. Tampoco la Unión Europea, más interesada en asuntos normativos y de privacidad que en los estratégicos y de seguridad. Este hecho esconde una clara declaración de intenciones y pone, una vez más, a Bruselas en una difícil situación al permanecer en la frontera del limbo cibernético y no asumir la dimensión estratégica que tiene el ciberespacio.

Ni la OTAN ni la Unión Europea son consideradas organizaciones fundamentales en materia cibernética.

Además, no se debe perder de vista que la integración y desarrollo de esta estrategia estadounidense se realizará en el marco de la Iniciativa de Innovación en Defensa que, considerada como el pilar tecnológico de la Tercera Estrategia de Compensación, pretende potenciar la investigación básica y aplicada, la cooperación de la industria y la atracción de expertos para mantener la supremacía militar y cibernética frente a cualquier adversario potencial presente y futuro. Y es que en línea con las lecciones aprendidas de la Revolución en los Asuntos Militares (RMA) que centró el planeamiento de la defensa durante la década de los noventa y que ofreció productos como los aviones invisibles, los drones o las armas de precisión, uno de los pilares tecnológicos de esta Estrategia de Compensación será el elemento cibernético, fundamental para la disuasión convencional y nuclear, la ciberguerra y para habilitar la conducción de operaciones militares.

En definitiva, con la nueva estrategia del Pentágono, EE UU ha puesto una nueva pieza en la construcción de su entramado de ciberdefensa y ha dado un paso más —si es que no existían ya suficientes indicios— para militarizar el ciberespacio. No descartemos que en los próximos meses veamos nuevos desarrollos y actuaciones en esta dirección.

At the end of last April, U.S. Secretary of Defense Ashton Carter presented the Pentagon's new cybersecurity strategy. Entitled "The DoD Cyber Strategy," this document, which replaces the strategy released in 2011, outlines the path to follow and the objectives to achieve in regard to cyber matters for the Department of Defense (DOD) during the period of 2015 to 2018. This is the first document of its kind that openly states that Washington will be able to perform cyberwar activities after claiming that the country "must be capable of resorting to cyber operations to destroy command and control networks, critical infrastructure or weapon systems of potential adversaries of the country."

The strategy also points out that cyber operations will be fully integrated into the planning and conducting of military operations. For this reason, in addition to promoting the creation of cyber capabilities conjointly, the Pentagon plans to create a cyberforce composed of 6,200 people organized into 133 teams whose main tasks are related to defense, intelligence, and attacks in cyberspace. Also, the DOD understands that the training and the career path of its cyberwarriors are inadequate. Therefore, the Pentagon has plans to develop exchange programs with the private sector, which has more advanced and adequate training programs.

Paradoxically, even though this strategy provides some ideas about how the cyber element can be used in joint military operations, it openly asserts that the U.S. will be able to utilize cyber capabilities in an offensive manner (and not only in cyberdefense or operational tasks after a cyberattack). In addition, the strategy briefly explicates the doctrine of deterrence and addresses the need to increase cooperation on matters of cybersecurity among the different administrations in the country, that is, between public and private actors and between key partners and allies.

This last aspect is very important, since it allows us to discover who Washington's allies are. On the one hand, there are the members of Five Eyes (Canada, Great Britain, Australia and New Zealand), followed by some countries in the Middle East and Asia-Pacific (which will be employed to support the third offset strategy in matters of defense) and some members of NATO. In other words, NATO, as an organization, is not considered a player in the matter due to the large deficiencies that some of the members have and which compromise its ability to perform. It should be noted that the cyber abilities of NATO meet the operational needs of a headquarters, command structure and partner agencies, and are available to its member nations if necessary. Neither is the European Union, which is more interested in legal and privacy issues than in strategic and security issues, considered a player. This fact conceals a clear statement of intentions, and it puts Brussels, once again, in a difficult situation, because it remains on the border of cyber limbo and does not assume the strategic dimension that cyberspace has.

Furthermore, one must not lose sight of the fact that the integration and development of this U.S. strategy will be carried out within the framework of the defense innovation initiative, which is considered the technological pillar of the third offset strategy and aims to promote basic and applied research, the cooperation of the industry, and the attraction of experts to maintain military and cyber supremacy against any potential, present or future adversary. And the matter is in keeping with the lessons learned from the Revolution in Military Affairs (RMA), a hypothesis which was involved in defense planning during the 90s and offered products like invisible aircraft, drones or precision weapons: that one of the technological pillars of this offset

strategy is probably the cyber element, which is essential for conventional and nuclear deterrence, cyberwar and to enable the conducting of military operations.

In short, with the Pentagon's new strategy, the U.S. has added a new piece in the construction of its cyberdefense structure and has taken one step further – if there was not sufficient evidence before – to militarize cyberspace. Let's not dismiss the idea that in the upcoming months we may see new developments and actions in this direction.