to 2012, oil imports from Nigeria dropped by more than 50%, from over 1 million to half a million barrels per day, and imports from Angola that were over half a million barrels per day in 2008 decreased to slightly less than 200,000 in 2012. Edward Morse, head of commodities research at Citigroup Global Markets, has predicted that, in 2014, the US and Canada will completely cease importing crude oil from West Africa.

This is a remarkable turn of events that is likely to have profound implications for US interests in sub-Saharan Africa. It will allow the US to adopt a more flexible and detached approach towards the region, especially in trouble areas such as Nigeria's onshore fields; the impact on oil exporting economies in western Africa will be widely felt as they adjust to rapidly changing energy trade flows. This is illustrated through the warning given by Nigeria's oil minister, Diezani Alison-Madueke, that increasing US production has become "one of the most serious threats to [sub-Saharan Africa's] producers," who stand to lose up to 25% of their oil revenue.

While the reduction in demand by the US for African energy exports might be significant in the short term, those exports will eventually be reoriented to supply emerging market demand, especially in the Asia Pacific region, where they can fetch high prices and demand is rapidly growing. Europe's role in sub-Saharan Africa's energy markets will remain marginal, as the EU's efforts to enhance energy security will be focused on relations with Russia and North Africa. Africa will become a somewhat more important source of global oil and gas production even as the continent's rapid economic growth – the phenomenon referred to as of "Africa Rising" – will result in decreased energy exports as local demand grows. This reorientation of African energy exports, from the West to the emerging markets of the Global South, will mirror shifts in political and other economic relations already under way, and most clearly demonstrated by the big imprint of China across the continent. Whether or not Africa will be able to better use the large and increasing revenues gained from energy exports to finance its own development, and thus to steer clear of the "resource curse" that has wreaked havoc across the continent, remains to be seen. As Paul Collier has forcefully argued, this question remains of key importance to Africa's future, just as African energy markets will remain of significance for those countries that will increasingly come to rely on African energy as a substantial supply source to meet their own demand. In that sense, Africa's role in the global economy remains, to some significant extent, defined by those natural riches that have so far constituted a decidedly mixed blessing for its inhabitants.

OPENING UP PANDORA'S BOX
CYBER SECURITY IN THE MENA ENERGY SECTOR

Justin Dargin
ENERGY AND MIDDLE EAST SCHOLAR,
UNIVERSITY OF OXFORD.

THE MIDDLE EAST-NORTH AFRICA (MENA) energy sector, which supplies over a third of the world's oil, and a significant amount of natural gas, is increasingly vulnerable to cyber-attacks. The rise in regional tensions, and the propensity for regional rivals to unleash cyber-attacks against each other's energy infrastructure compounds the threats to the global energy markets, both in terms of physically disrupting supply, and of injecting additional price volatility into the oil market.

The global energy sector, while at the forefront of the deployment of advanced technology in surveying and extraction, is woefully behind when it comes to protecting itself in cyber space. However, the greatest cyber threats to the energy sector must be clear. Broadly speaking, information technology security issues are related to two interrelated themes: cyber-attacks and cyber espionage. Neither one is a particularly recent phenomenon, for as soon as energy companies utilized computers on a large scale, techniques were developed to either attack these systems or to extract critical information. Cyber-attacks are geared towards disrupting or sabotaging processes within an energy company, while cyber espionage is focused on intellectual property theft. Most of the focus in the mainstream press raises the alarm over cyber-attacks, since it holds the potential to inflict massive damage to a company's, or country's ability to provide energy or power, so critical for day-to-day life. However, the theft of intellectual property, while not posing an immediate or catastrophic threat, can nonetheless cause long-term damage because the information gleaned may be used to perform a more devastating attack in the future.

Over the past several years, several high-profile cyber-attacks that targeted energy infrastructure struck the MENA region. In April/May 2012, the W32 Flame Virus attacked the National Iranian Oil Company (the second largest NOC in OPEC after Aramco) and the Iranian Oil Ministry. Furthermore, in August 2012, hackers launched cyber-attacks against the Saudi Arabian oil company Aramco and Qatari Natural gas producer RasGas through the use of the Shamoon Virus, also referred to as Disttrack. This malware is capable of overwriting computer files, which makes the targeted machine unusable.

The cyber-attack against Aramco infected nearly 30,000 workstations, erasing data on three-quarters of Aramco's computers. This ultimately purged documents, spreadsheets, e-mails, and files from the computer system. The virus replaced the purged files with an image of a burning American flag. The virus also siphoned data from the computers, sending it to a remote server. The U.S. Secretary of Defense, Leon Panetta, termed the attack "probably the most destructive attack that the private sector has seen to date."

The cyber-attack against RasGas was not as devastating as that against Aramco; it only took the company's website offline for a short period of time, and shut down some internal servers. As in both cases, since facilities are segmented behind a thick wall of cyber protection, the virus did not disrupt production. Whereas U.S. authorities suspect that Iran perpetrated the cyber-attacks, officials have not yet provided indisputable evidence supplementing that claim. In any case, it appears that insiders at Aramco, and possibly RasGas, facilitated entry for the hackers into the computer systems.

Because of the regional tensions associated with Gaza, Syria, the Arab Spring, as well as the tensions associated with the Iranian uranium enrichment program, which remains a highly combustible issue, it is likely that cyber-attacks in the region, focusing on energy infrastructure, will continue to expand

and increase in scope and sophistication. Many of the countries in the region are attempting to develop their own offensive and defensive capabilities in the sector. For instance, Qatar, Israel, Iran, the UAE, and Saudi Arabia are only a few of the MENA countries that are seeking to forge cyber capability to address an array of concerns. Moreover, as knowhow of the techniques necessary to conduct offensive cyber operations continues to spread, the threat to the MENA energy infrastructure will only increase. Additionally, as there are no international treaties governing cyber-attacks, there are no globally accepted and understood rules of what constitutes acceptable state action in this arena.

There are some wide-ranging impacts that can be expected from the increase in cyber related tension in the energy sector:

- As the energy-producing countries in MENA modernize their computer systems, their vulnerability to cyber-attacks will increase
- In light of recent attacks, most energy-producing Gulf countries invested significantly in network security. Some states, such as Qatar, are investing in potential offensive capability
- An significant attack on the computer network of an oil-producing country would have a definitive impact on energy markets, likely injecting a significant amount of volatility in the wake of any attack, notwithstanding whether the damage is long lasting or not;
- Since 2010, there have been approximately sixty significant reported cyber-attacks and cyber espionage incidents in the MENA region. Many of them remain unreported because of potential reputational damage; and
- If, as U.S. officials contend, Iran was behind the attacks in Gulf, and the denial of service (DoS) attacks on US financial institutions around the same time, possibly in retaliation against alleged Western attacks against Iranian computer infrastructure, it is nearly certain that cyber-attacks and espionage are going to increase in severity and scope in the mid-to-long term.

While there have been isolated cyber-attacks in the MENA region since the beginning of the 2000s, the start of hostilities can be traced to the unleashing of the Stuxnet virus, which targeted Iranian uranium enrichment facilities in 2010. Since then, several large-scale cyber-attacks, targeting critical infrastructure, have rippled throughout the MENA region. Some of the attacks are publicly known, at least five major cyber-attacks targeted critical infrastructure throughout the region; however, there have been other undisclosed attacks that have not been announced simply to keep national and corporate reputations intact.

Iran

Iran suffered several major computer attacks due to its efforts to create highly enriched uranium in the face of stiff international condemnation. The most damaging computer attacks against Iran began during the Bush Administration under a program code-named "Olympic Games" in which the US collaborated with Israel to create a sophisticated malware code to disrupt Iranian progress in its nuclear facilities, especially focused on the Natanz underground enrichment plant.

It appears that "Olympic Games" was the first time the US utilized cyber-attacks on a massive scale (outside of previous cyber-attacks with extremely limited aims) to disrupt another country's computer network.

When President Obama was elected in 2008, he continued the program, which became known to the public when a programing error caused it to escape the Natanz facility to the internet in the summer of 2010. Since its escape, it has infected millions of computers around the world, especially in China. After the Stuxnet attack, several other computer viruses compromised sensitive Iranian computer infrastructure. During April 2012, several waves of cyber-attacks targeted Iran's oil sector. These attacks did not seriously compromise Iran's oil production, as it is still primarily mechanical and not computerized. However, in a bid to mitigate the attack, Iranian officials disconnected several of its main oil terminals from the Internet to prevent the virus from spreading. In 2011, in order to provide defensive capabilities against further attacks, Iran formed a cyber-security wing with both a defensive and offensive mandate.

As a means to further protect its computer systems, Iran is planning to switch its citizens onto a domestic Internet system that will have limited interaction with global Internet infrastructure. The Iranian authorities already implemented the first phase, which connected all governmental offices and ministries to the national network. The second phase will focus upon bringing all nationwide Internet users into the national Internet fold. The Iranian government began to rollout the domestic Internet around March 2013, and officials have set a target date, over the next couple of years, for complete implementation of the program. While the election of the moderate politician, Hassan Al Rouhani, to the office of the president has ratcheted down "acute" tension with the West, there are still "chronic" disagreements with Western countries related to Iran's support of Palestinian groups, its role in Syria, its position toward the Gulf states, and its overall ideological stance, which considers the West as a hostile collective bent upon its destruction. That being the case, it can still be expected that Iran and the West will engage in covert cyber-related activity against each other's interests.

Saudi Arabia

The August 15, 2012 cyber-attacks against Aramco's network were the most destructive cyber-attack to date. The Shamoon virus deleted data on approximately 30,000 company computers, while it sent sensitive company information to network servers offline. As with the attacks against the Iranian oil facilities, Shamoon did not disrupt production, mostly because the main Aramco production facilities are behind a secure computer system, and much of the production technology is not completely computerized, but mechanized.

While Aramco did not publicly comment, US officials stated that they believe Iran was behind the attacks. Iran, for its part, denied any complicity. While Iran is widely assumed to have both the motive and the wherewithal to conduct the cyber-attacks, computer forensics is ongoing, at this stage, and no evidence indicating a perpetrator has been presented. Some evidence suggests that Iran perceived Saudi Arabia as engaging in economic warfare when the latter took advantage of reduced Iranian output during the summer of 2012 to increase its exports, and thus attacked Saudi Arabian production facilities in retaliation.

Preliminary evidence does point to the fact that individuals with privileged access to Aramco's facilities apparently facilitated the malware's entry into the system. Moreover, certain aspects of the code show that the malware had basic coding errors, which could be attributed to non-state actors. Several previously unknown groups took credit for the attacks, but it is not known whether these claims are legitimate. Furthermore, whether these alleged non-state actors were acting with the complicity and active guidance of state actors is also not yet definitively known.

Even before the attack on Aramco, Saudi Arabia was sufficiently concerned about potential computer breaches to double spending on homeland security, in early summer 2012, from $.7.8 billion to $15.4 billion. Saudi Arabia has also created a protection force for its oil sector, which will employ 35,000 personnel, with cyber security as the core focus.

Qatar

The attacks against RasGas occurred mere weeks after the Aramco attacks. However, the damage against RasGas, one of the world's largest natural gas companies, was minimal when compared to the number of servers affected in Saudi Arabia. The malware attack did not impact any aspect of RasGas' natural gas production. Qatar has been quite proactive in defining its cyber security posture, and had developed a dedicated governmental organization, in 2004, focused on deterring potential foes, as well as monitoring, detecting, and analyzing emergent cyber threats. Furthermore, after the attack on its energy sector, Qatar has taken steps to create an offensive cyber unit that would be able to target rival energy and computer networks, in the event of major hostilities.

The United Arab Emirates

While the UAE has not yet suffered a major cyber-attack against its energy infrastructure, it is concerned that it remains vulnerable. Typically, the UAE had to only consider cybercrime and hacking in terms of the many financial institutions that are located within its borders. Various reputable estimates posit that cybercrime costs the UAE approximately $600 million annually. While cybercrime and cyber-attacks/espionage are distinct, they tend to have overlapping methods of operation.

As a result of the early focus on financial security, the UAE had an early start in fortifying its network security. Due to these early efforts, according to an International Institute for Management Development (IMD) report, the UAE ranks first in cyber security in the region, and fourth globally.

In particular, as the UAE currently plans to increase its oil production from 2.8 million barrels per day to 3.5 million barrels per day by 2018, it is concentrating on developing a protective cyber security apparatus for its energy sector. Additionally, as the UAE is presently completing construction of its $20 billion nuclear power plants, it has invited cyber security companies to make certain that any potential attacks against its nascent nuclear sector will be nullified. This is of particular salience given the existence of malware such as Stuxnet, which was specifically produced to attack industrial and nuclear plants.

While other MENA countries are just now developing their cyber security infrastructure, the UAE federal authorities created the Telecommunication Regulatory Authority (TRA) to monitor the national information technology infrastructure, and provide suggestions on how to best forestall attacks. The TRA provides alerts to members and guidance on how to mitigate attacks. This is conducted through its Computer Emergency Response Team, which is a TRA initiative that is proactive in discovering structural weaknesses within the national computer network.

Cyber-Attacks Against MENA Energy Infrastructure: The Wave of the Future

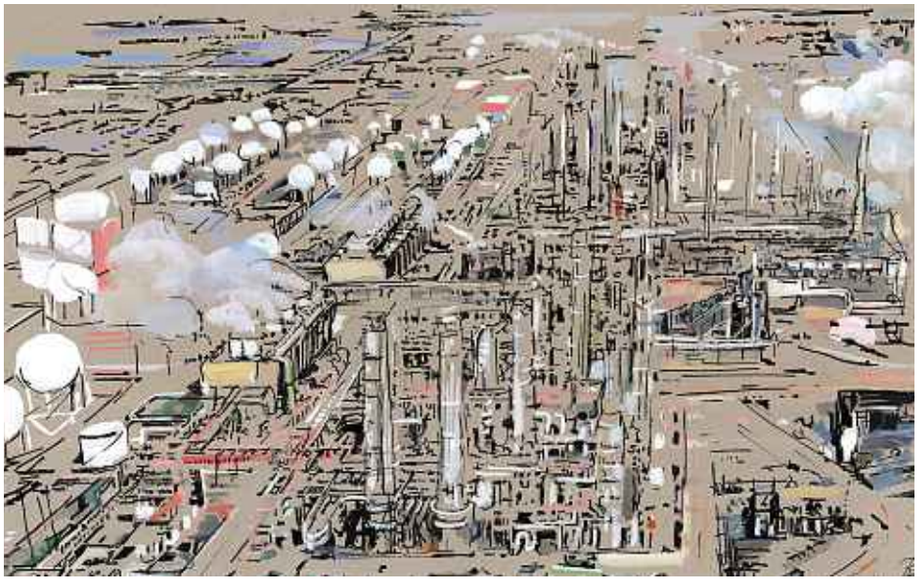
In all likelihood, cyber-attacks are going to increase significantly throughout the region, targeting not just governments, but also the financial sector (and therefore, private companies) and individuals. There are several reasons that cyber-attacks and espionage will increase exponentially in the future.

- Cyber-attacks are often viewed as a "cost-free" method to inflict damage on a rival, in that is it unlikely to invite a conventional military response.
- Often cyber-attacks are not disclosed due to embarrassment to companies. Therefore, it may be difficult to understand whether several coordinated cyber-attacks are underway and provide effective counter measures.
- It is often difficult to discover the identities of the perpetrators of the cyber-attack.
- Western countries decided to utilize cyber-attacks as one of the main methods forestall and disrupt the development of the Iranian nuclear program. This new method of sabotage has invited retaliation of a similar nature as countries in the region have decided to invest in their own cyber warfare capabilities.
- The increasing regional tension due to overall tension between Iran and the West, as well as Syria and the associated Arab Spring turmoil, increased not only the threat of cyber-attacks, but also the likelihood that both non-state actors and states will view it as a legitimate means to undermine regional rivals.

When the U.S. initiated cyber-attacks and espionage against Iran as a means to disrupt its uranium enrichment program, it opened up a veritable Pandora's Box in the region, increasing the possibility of the use of such asymmetric warfare. Additionally, the U.S. often sets the tone for what is globally acceptable. In this sense, while the short-term interests of disrupting Iranian progress on its uranium enrichment plans are viewed as being paramount, when cyber-attacks are utilized as a viable policy against rivals, it allows other actors to develop and use the technology without hesitation. This has given pause to U.S. authorities while they continue to map out a coherent cyber-security policy to deal with emergent threats in the MENA region. The region remains vulnerable to threats that can emanate from several quarters, such as:

- Organized criminal syndicates, which can be hired to undertake cyber-attacks and are primarily interested in financial gain;
- Ideologically oriented groups that are not sponsored by state actors. This group includes "hacktivists" (e.g., Anonymous) who attacked Israeli networks during the Gaza conflict; and
- State-sponsored groups that work under the auspices of hostile state powers.

Escalation of successful cyber-attacks against MENA energy companies would have a destabilizing effect on the entire region that would cascade throughout the world energy markets in the form of a decrease in oil and natural gas supply, and an increase in prices. Even if targeted cyber-attacks against regional energy infrastructure were not successful in disrupting energy production, it would still impact international energy prices, especially that of oil. In the wake of any significant cyber-attack, successful or unsuccessful, price volatility would increase.



"NEW" NUCLEAR ENERGY

Sharon Squassoni

SENIOR FELLOW & DIRECTOR, PROLIFERATION PREVENTION PROGRAM CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

NUCLEAR ENERGY TODAY GENERATES about 10% of global electricity. The prospects for increasing that share are dim: nuclear power's share of commercial electricity generation may have peaked more than twenty years ago at 17%.[1] This contrasts sharply not only with rhetoric about a nuclear renaissance, but also with trends for renewable energy, which are clearly moving along an upward trajectory. At least two factors will make it difficult for nuclear energy to play a leading role in electricity generation: its own growth will be quickly outpaced by overall electricity demand (expected to double by 2050), and existing capacity will require replacement even as industry adds new capacity elsewhere.

Still, nuclear energy has hung on for fifty years, enduring major accidents (Chernobyl and Fukushima), resource concerns, rising construction costs, and the unresolved problems of waste, nuclear terrorism, and nuclear proliferation. Nuclear energy will likely continue to hang on over the next fifty years, with a few small changes.

A New Look for Nuclear

First, nuclear power will expand to new regions. It will shift from the developed countries to the developing countries, and from Europe to Asia. Some growth may be possible in the Middle East, and in Africa.

For decades, nuclear power plants have been located predominantly in developed countries. In 2011, six countries (the United States, France, Japan, Russia, South Korea, and Germany) generated more than 70% of all nuclear electricity. Not only is Germany getting out of nuclear energy, but the future in Japan is also uncertain, after the Fukushima accident in 2011.[2] Several other countries – Belgium, Taiwan, the Netherlands, Switzerland – have indicated they would gradually phase out nuclear power.

Asia, on the other hand, will fill some gaps, but not all. China is building 29 of the 69 units worldwide that are under construction. India and South Korea have robust construction plans, but both are experiencing delays. Vietnam will build a handful of reactors, and Indonesia and Malaysia are considering their options.

In the Middle East, the United Arab Emirates plans to build ten nuclear power reactors, having awarded a contract in 2009 to Korea Electric Power Company (KEPCO) for four units. Jordan, Morocco, Saudi Arabia, Oman, Qatar, and Bahrain all are interested in nuclear power, but apart from Saudi Arabia, none is likely to build more than one or two reactors. Elsewhere, developing countries such as Bangladesh, Indonesia, and Malaysia in Southeast Asia, Azerbaijan, and Belarus in Central Asia, and Nigeria, Kenya, Ghana, and Tunisia in Africa also have expressed interest in nuclear power.

A second shift may be in the kinds of nuclear power plants deployed. Developing countries mostly lack the electricity grid infrastructure to support the size of nuclear power plants that are now most commonly marketed (1000MWe to 1500MWe range). Small modular reactors may be appealing, but few so far are licensed and ready to be built. This category of reactors can include tiny 10MWe reactors, floating reactors, or larger 200-600MWe more traditional designs. Part of the problem in developing reactors specifically for new environments is that users are hesitant to buy a design that has not been in operation elsewhere. With demand declining in the developed world, it may be tougher for nuclear suppliers to prove their credentials by building and operating such reactors in existing markets.

A third shift is in nuclear governance. This has been a moving target, even in the developed world, with tighter regulations for safety, security, and nonproliferation imposed only after significant accidents and incidents. In the developing world, where governance in general is poor, the intensive process required to put in place the entire regulatory and legal framework necessary for operating a safe, secure nuclear power may be particularly challenging. There is an alarming overlap between countries that are interested in nuclear power for the first time and significant governance challenges. Figure 3 shows this overlap with Foreign Policy's Failed State Index. One solution is to have suppliers supply more than just nuclear power plants. In fact, recipients are increasingly interested in contracts that

La seguridad cibernética
abriendo la caja de Pandora en Oriente Medio y norte de África

Justin Dargin
ESPECIALISTA EN ENERGÍA Y ORIENTE MEDIO, UNIVERSIDAD DE OXFORD.

EL SECTOR ENERGÉTICO DE LA REgión de Oriente Medio y Norte de África (MENA, por sus siglas en inglés), que suministra más de un tercio del petróleo mundial y una cantidad importante de gas natural, es cada vez más vulnerable a los ataques cibernéticos. El aumento de la tensión en la región y la propensión de los distintos países a lanzar ataques cibernéticos contra infraestructuras energéticas rivales amenazan los mercados mundiales de la energía, tanto en términos de interrupción física del suministro como de inestabilidad en los precios de mercado del petróleo.

El sector global de la energía, aunque se halla a la vanguardia en cuanto a tecnologías avanzadas de prospección y extracción, se queda lamentablemente atrás cuando se trata de protegerse a sí mismo en el ciberespacio. Debe aclararse, no obstante, cuáles son las principales amenazas para el sector de la energía en el ámbito cibernético. En términos generales, los problemas de seguridad relacionados con las tecnologías de la información tendrían que ver con dos cuestiones vinculadas entre sí, como son los ataques y el espionaje cibernéticos. Ninguno de los dos representa un fenómeno particularmente reciente, ya que tan pronto como las compañías de energía empezaron a utilizar los ordenadores a gran escala, se desarrollaron técnicas para atacar estos sistemas o para extraer de ellos información crucial. Los ciberataques están dirigidos a interrumpir o sabotear los procesos dentro de una empresa de energía, mientras que el espionaje cibernético se centra en el robo de la propiedad intelectual. Los principales medios de comunicación han tratado de hacer sonar la alarma sobre los ataques cibernéticos, aludiendo a su potencial para causar daños masivos en la capacidad de una empresa o de un país en un área tan importante como el suministro de energía. Si bien el robo de propiedad intelectual no presenta una amenaza inmediata o catastrófica, puede no obstante causar daños a largo plazo, dado que la información obte-

> El sector de la energía, que dispone de tecnologías de vanguardia para la prospección y la extracción, es vulnerable a los ataques y al espionaje cibernético, en especial en Oriente Medio y norte de África

nida puede ser utilizada para llevar a cabo un ataque más devastador en el futuro.

En los últimos años, la infraestructura energética de la región MENA ha sufrido importantes ataques cibernéticos. En abril-mayo de 2012, el virus W32 Flame atacó a la Compañía Nacional Iraní de Petróleo (el segundo mayor centro de operaciones de red de la OPEP después de Aramco) y al ministerio iraní del Petróleo. Por otra parte, en agosto de 2012, la empresa petrolera saudí Aramco y la compañía productora de gas natural qatarí, RasGas, sufrieron sendos ataques cibernéticos por parte de los piratas informáticos. Éstos se sirvieron para ello del virus Shamoon, también conocido como Disttrack, un *malware* (software malicioso) capaz de sobreescribir archivos informáticos e inutilizar un ordenador.

La situación política en la región de los países del MENA sigue siendo altamente inestable, y es probable que los ataques cibernéticos continúen extendiéndose e incrementando su alcance y sofisticación

El ciberataque contra Aramco infectó casi 30.000 ordenadores y borró los datos de las tres cuartas partes de aquéllos. En definitiva, destruyó documentos, hojas de cálculo, correos electrónicos y archivos del sistema operativo. El virus reemplazó los archivos afectados por la imagen de una bandera estadounidense en llamas, además de desviar datos enviándolos a un servidor remoto. El secretario de Defensa de Estados Unidos, Leon Panetta, calificó el ataque como "probablemente el más devastador sufrido por el sector privado hasta la fecha".

El ciberataque contra RasGas no fue tan destructor como el sufrido por Aramco, pues sólo dejó sin conexión el sitio web de la compañía durante un rato y bloqueó algunos servidores internos. El virus no interrumpió en ningún caso la producción, ya que las instalaciones se hallaban protegidas por un grueso muro de seguridad cibernética. Aunque las autoridades estadounidenses sospechan que fue Irán el que perpetró los ataques cibernéticos, los medios oficiales aún no han proporcionado pruebas irrefutables que confirmen tal afirmación. En cualquier caso, parece que fueron empleados de Aramco y, posiblemente, de RasGas, con acceso autorizado a los datos, quienes franquearon a los piratas la entrada a los sistemas informáticos de estas empresas.

Debido a las tensiones existentes en Gaza y Siria, así como a las revueltas de la *primavera árabe*, y a pesar de que el conflicto relacionado con el enriquecimiento de uranio por parte de Irán está en vías de resolverse, la situación sigue siendo altamente inestable y es probable que los ciberataques en el sector energético continúen extendiéndose y ganando alcance y sofisticación. Muchos de los países de la región se están centrando en desarrollar sus propias capacidades ofensivas y defensivas en el sector. Por ejemplo, Qatar, Israel, Irán, los Emiratos Árabes Unidos y Arabia Saudí son sólo algunos de los países de MENA que están tratando de perfeccionar su capacidad cibernética a fin de poder afrontar posibles desafíos en el futuro. Además, como los conocimientos de las técnicas necesarias para llevar a cabo ofensivas cibernéticas continúan esparciéndose, la amenaza a la infraestructura energética de MENA será cada vez mayor. Asimismo, ya que no existen tratados internacionales que rijan las respuestas y actuaciones ante los ciberataques, tampoco se han consensuado unas reglas generales para la actuación del Estado en esta materia.

Podemos citar algunos impactos de amplio alcance relacionados con el aumento de la tensión originado por la actividad cibernética en el sector de la energía:

- En la misma medida en que los países productores de energía en la región MENA modernicen sus sistemas informáticos, también se incrementará su vulnerabilidad a los ataques cibernéticos.

- A la luz de los recientes ataques, la mayoría de los países productores de energía del Golfo han invertido de forma importante en seguridad de red. Algunos países, como Qatar, están invirtiendo en capacidad ofensiva.

- Un ataque importante a la red informática de un país productor de petróleo tendría un impacto definitivo sobre los mercados energéticos, probablemente desestabilizando los precios, independientemente de si el daño causado es duradero o no.

- Desde el año 2010 se han producido aproximadamente 60 casos importantes de ciberataques e incidentes de espionaje cibernético en la región MENA, muchos de los cuales no se han hecho públicos a fin de evitar un posible daño a la reputación del sector.

- Funcionarios estadounidenses sostienen que Irán estaba detrás de los ataques en el Golfo y

de la denegación de servicio (DoS, por sus siglas en inglés) contra instituciones financieras de Estados Unidos, posiblemente en represalia por los presuntos ataques por parte de Occidente contra su infraestructura informática. Es de prever, por tanto, que los ciberataques y el espionaje vayan aumentando su intensidad y alcance a medio y largo plazo.

Si bien se han producido ataques cibernéticos aislados en la región MENA desde principios de la década de 2000, el comienzo de las hostilidades podría situarse en el momento del ataque de los virus Stuxnet dirigido contra las instalaciones iraníes de enriquecimiento de uranio en 2010. Desde entonces, los ataques cibernéticos a gran escala se extendieron por toda la región MENA. Algunos de ellos han sido reconocidos públicamente, al menos cinco grandes ataques dirigidos contra infraestructuras importantes en la región. Otros, sin embargo, no han sido jamás revelados, simplemente para mantener intacta la reputación nacional y empresarial.

Irán

Irán sufrió varios ataques cibernéticos importantes en respuesta a sus actividades encaminadas a crear uranio enriquecido y hubo de hacer frente a un severo oprobio internacional. Los ataques informáticos más dañinos contra Irán comenzaron durante la Administración Bush con un programa denominado en clave *Juegos Olímpicos*, en el que Estados Unidos e Israel colaboraron para crear un sofisticado código de *malware* destinado a interrumpir el progreso iraní en sus instalaciones nucleares, especialmente en la planta de enriquecimiento de Natanz.

Al parecer, fue con el programa *Juegos Olímpicos* cuando Estados Unidos empleó por primera vez los ciberataques a gran escala –exceptuando ataques cibernéticos anteriores con objetivos muy limitados– para trastocar la red informática de otro país.

Cuando fue elegido el presidente Obama en 2008, continuó con el programa, que llegó a hacerse público cuando un error de programación lo hizo saltar a internet en el verano de 2010. Desde entonces, el virus ha infectado a millones de ordenadores en todo el mundo, especialmente en China. Después del ataque Stuxnet, otros virus informáticos comprometieron la sensible infraestructura informática iraní. Durante el mes de abril de 2012, varias oleadas de ataques cibernéticos apuntaron contra el sector petrolero de Irán. Estos ataques no comprometieron seriamente la producción de petróleo, que sigue siendo principalmente mecánica y no informatizada. Sin embargo, en un intento por mitigar el ataque, los funcionarios iraníes desconectaron varios terminales petroleros principales para evitar la propagación del virus. Con el fin de poder contrarrestar nuevos ataques, Irán organizó en 2011 un proceso dual de creación de un ala de seguridad cibernética con mando defensivo y ofensivo.

Con el objetivo de proteger aún más sus sistemas informáticos, Irán tiene la intención de instaurar para sus ciudadanos un nuevo sistema de internet que opere a nivel interno y que tendrá una interacción limitada con la infraestructura global. Las autoridades iraníes ya pusieron en práctica la primera fase, que conecta todas las oficinas gubernamentales y ministerios a la red nacional. La segunda fase se centrará en lograr que todos los usuarios de internet de todo el país adopten este nuevo entorno de red nacional. El gobierno iraní comenzó a desarrollar esta red interna alrededor de marzo de 2013 y ha fijado como fecha límite el plazo del próximo par de años para la ejecución completa de todo el programa. Si bien la incorporación del político moderado Hasan Rohani a la oficina del presidente ha reducido la *aguda* tensión con Occidente, todavía existen desacuerdos *crónicos* con los países occidentales relacionados con el apoyo de Irán a los grupos palestinos, con su papel en Siria, con su posición hacia los países del Golfo y con su postura ideológica general que considera a Occidente como un colectivo hostil que busca su destrucción. Por lo tanto, todavía cabe esperar que Irán y Occidente continúen intentando minar mutuamente sus intereses a base de actividades cibérneticas encubiertas.

Durante el mandato de Georges W. Bush, Estados Unidos e Israel lanzaron el primer ciberataque ('Juegos Olímpicos') a gran escala contra Irán para interrumpir su programa de enriquecimiento de uranio

Arabia Saudí

El 15 de agosto de 2012, el ciberataque a la red de Aramco fue el más destructivo ocurrido hasta la fecha. El virus Shamoon eliminó datos de aproximadamente 30.000 ordenadores, desconectando además los servidores de red de la empresa. Al igual que con los ataques a las instalaciones petrolíferas iraníes, Shamoon no interrumpió la producción debido principalmente a que los principales

centros de producción de Aramco se hallan protegidos por un seguro sistema informático y a que gran parte de la producción se encuentra mecanizada y no completamente informatizada.

Aunque Aramco no hizo ninguna declaración, funcionarios estadounidenses afirmaron que creían que Irán se hallaba detrás de los ataques. Irán, por su parte, negó cualquier tipo de implicación en el asunto. Si bien existe la creencia generalizada de que Irán cuenta tanto con la motivación como con los medios para llevar a cabo tales ataques, la investigación se halla en curso y no se han presentado pruebas que indiquen que Irán perpetró los atentados. Algunas pruebas sugieren que, debido a que Arabia Saudí se aprovechó de la reducción de la producción iraní durante el verano de 2012 para aumentar sus exportaciones, Irán, que consideró ese hecho como una guerra económica, atacó las instalaciones de producción de Arabia Saudí en un intento de castigo. Las pruebas preliminares descartarían la posibilidad de que personal con acceso privilegiado a las instalaciones de Aramco estuviera implicado en la entrada del *malware* en el sistema. Además, parece que ciertos segmentos del código indican que el *malware* presentaba errores básicos de codificación que podrían ser atribuidos a agentes no gubernamentales. Previamente, varios grupos desconocidos se atribuyeron los ataques, pero no hay certezas al respecto. Por otra parte, si estos presuntos agentes no gubernamentales actuaban con la complicidad y orientación activa por parte de la Administración, no es tampoco algo que se sepa hasta el momento.

Los Emiratos Árabes Unidos, pioneros en reforzar la seguridad de sus redes, es el país mejor protegido de la región y el cuarto en todo el mundo; destina unos 600 millones de dólares al año en ciberdefensa

Antes incluso del ataque contra Aramco, Arabia Saudí estaba bastante concienciada acerca de estos posibles ataques informáticos, ya que duplicó el gasto en seguridad nacional a principios del verano de 2012, pasando la partida presupuestaria dedicada a este sector de 7.800 a 15.400 millones de dólares. También ha creado un cuerpo de protección para su sector petrolero, que dará empleo a 35.000 personas y está enfocado principalmente a la seguridad informática.

Qatar

Los ataques contra RasGas ocurrieron en cuestión de semanas después de los ataques a Aramco. Sin embargo, el daño contra RasGas, una de las mayores empresas de gas natural del mundo, fue mínimo en comparación con el número de servidores afectados en Arabia Saudí. El ataque de *malware* no afectó ningún aspecto de la producción de gas natural de RasGas. Qatar ha sido bastante previsor con respecto a su postura en seguridad cibernética y desarrolló en 2004 una organización gubernamental orientada a la disuasión de potenciales enemigos y a la vigilancia, la detección y el análisis de amenazas informáticas emergentes. Por otra parte, tras el ataque a su sector energético, Qatar ha adoptado medidas para la creación de una unidad cibernética ofensiva capaz de atacar las redes informáticas rivales en caso de que inicien hostilidades.

Emiratos Árabes Unidos

Aunque los Emiratos Árabes Unidos no han sufrido ningún ciberataque importante contra su infraestructura energética, su vulnerabilidad sigue siendo preocupante. Este país ha tenido, sin embargo, que afrontar la ciberdelincuencia y la piratería en buena parte de sus instituciones financieras. Según fuentes fidedignas, el ciberdelito le cuesta a los EAU en torno a 600 millones de dólares anuales. Aunque el ciberdelito y el ciberataque/espionaje son acciones distintas, ambas tienden a coincidir en métodos operativos.

A consecuencia del enfoque adoptado por los EAU respecto a su seguridad financiera, este país fue pionero en reforzar la seguridad de sus redes. Debido a estos precoces esfuerzos, y de acuerdo con un informe del Instituto Internacional para el Desarrollo Gerencial (IMD, por sus siglas en inglés), ocupan el primer lugar en seguridad cibernética en la región y el cuarto a nivel mundial.

En concreto, los Emiratos Árabes Unidos tienen previsto actualmente aumentar su producción de petróleo para el año 2018 de 2,8 a 3,5 millones de barriles diarios, por lo que se está concentrando en el desarrollo de un sistema de seguridad cibernética que proteja su sector energético. Además, al estar finalizando la construcción de sus centrales nucleares (por valor de 20.000 millones de dólares), ha reunido a las empresas de seguridad cibernética para asegurarse de que todos los posibles ataques contra su incipiente sector nuclear quedan invalidados. Esto tiene sentido especialmente si se tiene en cuenta la existencia de *malware* como Stuxnet, específicamente diseñado para atacar las plantas industriales y nucleares.

Mientras que otros países de la región MENA están ahora desarrollando sus infraestructuras de seguridad cibernética, las autoridades federales de

los Emiratos Árabes Unidos han creado la Autoridad Reguladora de las Telecomunicaciones (TRA, en inglés). Este organismo se encarga de supervisar la infraestructura nacional de tecnologías de la información, proporciona alertas a los miembros, da indicaciones sobre cómo prevenir mejor los ataques y aconseja cómo mitigarlos. Esto se lleva a cabo a través del Equipo de Respuesta a Emergencias Informáticas, una iniciativa de la TRA que se encarga de estudiar las debilidades estructurales de la red informática nacional.

Los ciberataques contra la infraestructura energética MENA: las señales del futuro

Con toda probabilidad, los ciberataques aumentarán de forma importante en toda la región, apuntando no sólo a los gobiernos, sino también al sector financiero (y por lo tanto a las empresas privadas) e, incluso, a personas físicas. Varias razones explicarían este aumento exponencial previsto de los ciberataques y el espionaje en el futuro:

- Los ciberataques son considerados generalmente como un método *sin coste* para infligir daño a un rival, con escasa probabilidad de suscitar una respuesta militar convencional.

- A menudo, los ataques cibernéticos no son revelados debido a la vergüenza que de ello resulta para las empresas. Por lo tanto, su detección es complicada si están en marcha varios ataques cibernéticos coordinados, lo que impide que puedan adoptarse medidas eficaces en contra.

- En general, no es tarea fácil identificar a los perpetradores de los ataques cibernéticos.

- Los países occidentales decidieron utilizar los ciberataques como uno de los métodos principales para prevenir e interrumpir el desarrollo del programa nuclear iraní. Este nuevo método de sabotaje ha provocado represalias de naturaleza similar de modo que los países de la región decidieron invertir en su propio potencial *cibermilitar.*

- El incremento de las tensiones en la región a causa del conflicto de Occidente con Irán, pero también del de Siria y el relacionado con los sucesos de la *primavera árabe,* no sólo hizo aumentar la amenaza de ataques cibernéticos, sino que supuso también una ocasión para que agentes estatales y no estatales consideraran legítimo socavar los intereses de sus rivales en la región.

Cuando Estados Unidos inició sus ataques cibernéticos y el espionaje contra Irán como medio para interrumpir su programa de enriquecimiento de uranio, se abrió una verdadera caja de Pandora en la región, ya que aumentó así la posibilidad de escalada de dicha guerra asimétrica. Además, Estados Unidos suele marcar la pauta de lo que es aceptable o no a nivel mundial. En este sentido, desde el momento mismo en que sus intereses a corto plazo de interrumpir el progreso de Irán sobre sus planes de enriquecimiento de uranio son considerados de suma importancia, se está dando vía libre a otros países para que desarrollen y usen la tecnología sin grandes vacilaciones. Esto ha hecho reflexionar a las autoridades estadounidenses al tiempo que continúan desarrollando una política coherente de seguridad cibernética capaz de hacer frente a las amenazas emergentes en la región MENA. La zona sigue siendo vulnerable a las amenazas, que pueden emanar de sectores tales como:

- Organizaciones criminales, que pueden ser contratadas para llevar a cabo ataques cibernéticos y cuyo interés principal es obtener beneficio económico.

- Grupos ideológicos no relacionados con agentes gubernamentales. Se incluyen aquí los *hacktivistas* (por ejemplo, Anonymous) que atacaron las redes israelíes durante el conflicto de Gaza.

- Grupos que funcionan bajo el auspicio de poderes estatales hostiles.

La escalada de éxito de los ataques cibernéticos contra las empresas energéticas de la región MENA tendría un efecto desestabilizador en toda la región. Los mercados mundiales de la energía se verían afectados por una disminución en el suministro de petróleo y gas natural y por un aumento de los precios. Incluso si los ciberataques dirigidos contra la infraestructura energética regional no lograran interrumpir la producción de energía, seguirían aún afectando a los precios mundiales de la energía, especialmente en el caso del petróleo. A raíz de cualquier ataque cibernético importante, exitoso o no, aumentaría la inestabilidad de los precios.