INSS Insight No. 646, December 23, 2014

Cyberspace Extortion: North Korea versus the United States

Gabi Siboni and David Siman-Tov

The announcement by Sony Pictures that it would not release *The Interview* for screening in major US theaters as planned was the culmination of a series of events that featured elements of cyber warfare and psychological warfare, and threatened to spill over into physical terrorism. The incident occurred where the worlds of policy and of culture converge, namely, politics. The implication of this extraordinary affair goes far beyond a North Korean conflict with Sony and the United States; it even goes beyond economics, though the wave of attacks caused the Sony Corporation tremendous financial losses in addition to the direct damage resulting from the decision not to distribute the movie. At stake is a fundamental value of the West in general and the United States in particular – the right of free speech.

The purpose of the attack, attributed to North Korea, was to deter Sony Pictures from releasing the movie, which was understood (correctly) as ridiculing that country's dictator and portraying the North Korean regime and its leader, Kim Jong-Un, with sarcasm and mockery. At first, North Korea reacted via diplomatic channels in an attempt to prevent the movie's distribution and screening. It subsequently announced that as far as it was concerned, screening the movie was a declaration of war that would not be ignored or tolerated. Under pressure, Sony altered the script in an effort to lessen the scorn, but Pyongyang was not mollified. As the production of the movie progressed and reached the point of distribution, Sony became the target of a wave of cyberattacks that climaxed when personal data of company employees, such as salaries, Social Security numbers, and emails were made public; company servers and computers were hacked, interrupting work at the company for about a week; and scripts and various versions of new movies in production at Sony were leaked to the internet.

The attacks were most likely carried out by a group of hackers calling themselves the Guardians of Peace. Although North Korea is an isolated nation with little internet access, it is believed to have highly developed cyber capabilities. Indeed, the attack against Sony supports that assessment of the nation's cyberspace know-how, already demonstrated in cyberattacks against South Korea, for example.

Sony's helplessness is typical of all systems in the United States in particular and the West in general, and reflects the limited ability by Western democracies to repel attacks of this kind. Attacks on private companies and corporations for the sake of industrial and political espionage are common. They are carried out by state-sponsored entities, hacker groups supported and instructed by states, and by criminal organizations. But it is possible that the events surrounding Sony's movie point to an especially menacing trend with novel features: the use of cyberspace combined with the threat of physical harm, and the state not denying responsibility for the attacks and threats.

The current cyberattack integrated pressure on a private company and cyberspace threats against it with the threat of physical harm to civilians. To enhance the deterrence, the threats to harm the movie's distributors and moviegoers included the exhortation "Remember September 11." Various ideas for physically securing the movie houses that might screen *The Interview* in the future have been floated, but it is still unclear how Sony will act and if North Korea has other cyber weaponry in its arsenal. Whether North Korea would have tried to realize its threats of physical damage had Sony decided to launch the movie is unknown; to do so would require very specific and complex operational capabilities. In any case, thus far North Korea has scored a noteworthy psychological victory.

Moreover, given the difficulty in identifying hackers, assessments as to their identity are speculation alone. To date, state-sponsored attacks on the private sector for the purpose of industrial espionage and information theft have been attributed primarily to China. However, in this sense, the attack on Sony was unusual: at first, the North Korean regime did not deny responsibility for the attack carried out by hackers identified with the regime. Hints as to its involvement were broadcast in North Korean media. The explanation seems to be that North Korea is seeking to create an explicit equation of deterrence in case of future attempts to jeer at the nation and its ruler. Indeed, the relative weakness of Western democracies in the cyberspace battlefield was quite apparent. President Obama addressed the issue, albeit somewhat belatedly, complaining that Sony executives had not consulted him before making their decision. He said the United States would not agree to any curtailment of freedom of speech, and promised it would choose the time and manner of its response. But it seems that the North Korean regime is not worried about a response, cyber or physical, on the part of the United States.

States and organizations potentially interested in limiting the right to freedom of speech and action of other states and organizations are no doubt watching events closely and are liable to act on the conclusions drawn from the North Korea versus Sony Pictures affair. While the specific incident focused on the film industry, presumably other sectors are equally exposed to damage, including civilian business sectors that are not at the top of any state's cyber protection and defense agenda.

One of the unfortunate conclusions arising from this incident is the emerging trend of exploiting cyberspace capabilities for the sake of political extortion. The implications are liable to exceed the limits of free speech. As the unfolding of the affair made clear, attacks of this kind have the strong tendency to go outside the business arena and involve political echelons and governments. In other words, the incident demonstrates the realization of a threat imagined in the past, in which cyberspace becomes yet another battleground among the nations of the world.