Centre for Air Power Studies (CAPS)
Forum for National Security Studies (FNSS)

U.S. PROPOSES ECONOMIC SANCTIONS AGAINST CHINA OVER CYBER THEFTS: ITS EFFECTIVENESS, VIABILITY AND LEGITIMACY

Gp Capt Ashish Gupta
Senior Fellow, CAPS

Sanctions – predominately economic and peripherallypolitical and military, constitute an important element of foreign policy. Sanctions, against a state or an entity, are employed as coercive instruments to elicit a behavioral change or to diminish belligerent posturing. In the post-cold war era, the waning reliance onarmed conflicts and wars, within and among states, for resolution of belligerent, contentious and complex problems has resulted in widespread use of economic sanctions. Sanctions have been used in support of foreign policy goals:to discourage armed aggression, cap the aspirations of potential nuclear states, rein in drug trafficking, expedite political change, discourage proliferation of weapons of mass destructions and dissuade support for terrorism.

Some political observers and decision makers think of sanctions as a measured and proportionate response to a challenge considered below the threshold of perceived national interests at stake. In addition, sanctions can be considered asa form of expression or message-sending to communicate disapprobation of a particular action or behavior. It was appropriately observed by America's Catholic bishops that "Sanctions can offer a nonmilitary alternative to the terrible options of war or indifference when confronted with aggression or injustice."[1]

In order to gauge the efficacy of economic sanctions and ascertain the underlying rationale, the analysis of sanctions against Iran provides some perspectives. In case of Iran, in order to cap itssupposedly illicit nuclear activities, the U.S., the member states of the European Union and others put in place a strong, inter-locking matrix of sanctions measures relating to Iran's nuclear, missile, energy, shipping, transportation, and financial sectors.[2] The EU embargo and the U.S. sanctions played havoc with Iranian national economy. Iran's oil exports fell drastically and in

January 2013, Iran's oil minister acknowledged that the fall in oil exports was costing the country between U.S. $4billion and U.S. $8 billion each month. Iran is believed to have suffered a loss of about U.S. $26 billion in oil revenue in 2012 from a total of U.S. $95 billion in 2011. In April 2013, the International Monetary Fund (IMF) forecast that Iran's gross domestic product (GDP) would shrink by 1.3% in 2013 after contracting by 1.9% the previous year.

In exchange for Iran's commitment to limit its nuclear capabilities and its pledge to limit its nuclear energy activities for purely peaceful purposes, the United Nations Security Council, on July 20, unanimously approved a resolution that created the basis for international economic sanctions against Iran to be lifted.[3]

Buoyed bydegree of success, albeit still speculative, as a result of sanction measures against Iran, the Obama administration, is in the process of buttressing similar tenets in an entirely different domain. The U.S., wary of cyber economic espionage initiated by Chinese hackers perhaps with the tacit approval and support of Chinese government has suffered enormous monetary losses as well as loss of intellectual property and prestige. Securing cyberspace represents the Holy Grail of "National Security."In response to the rising wave of cyber-attacks exponentially growing in numbers and the potential severity of subsequent consequences, the U.S. is putting in place a framework intended to subject Chinese companies and individuals to unprecedented economic sanctions, who have been direct or incidental beneficiaries of U.S. trade secrets through cyber theft by Chinese governments.[4]

The provision of sanctions against Chinese companies and individuals, once enacted and established as expedient, would mark the far-reaching use of Executive Order signed by President Barack Obama in April 2015. The executive order, "Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities", identifies increasing prevalence and severity of malicious cyber enabled activities originating from, or directed by persons located, in whole or in substantial part, outside the United States as an unusual and extraordinary threat to the national security, foreign policy, and economy of the United States.[5] The EO explicitly specifies blockage of all property and interests in property in the U.S. of persons responsible for or engaged, either directly or indirectly, cyber-enabled activities.

This U.S. move is being described as the second serious and important shot at deterring the China on the issue of cyber espionage. Last year, in May, in a first-of-its-kind case, U.S. Justice Department indicted five Chinese military officers on charges of stealing data from six U.S. companies. The U.S. formally accused Chinese officers and sought their extradition to face charges under U.S. laws for infiltrating the computer networks of six U.S. companies and for stealing data, which could be leveraged for the

benefits by their trade competitors. The FBI had gone to the extent of putting the faces of five officials on 'Wanted' poster.[6]

However, some U.S. officials within the government caution against such moves and question the overall efficacy in the long run, arguing that sanctions might exacerbate tensions in already tumultuous diplomatic relations between the United States and China. Besides, the U.S. can't take moral high ground when the U.S. itself is accused of perpetrating cyber espionage, mass surveillance and other forms of information gathering directed at its allies and adversaries. The whole exercise orchestrated by US appears to be an attempt to "send a strong message" to Beijing, though China is not likely to buckle under pressure from supposedly strong arm tactics of US.

Economic sanctions alone will not bring in a paradigm change in the Chinese behavior. A nation's resolve to deter cyberattacks needs to be part of its overarching defencestrategy encompassing all instruments of national power-diplomatic, economic, informational and military. The anonymity and impunity, with which the acts of cyber terrorism and espionage are being carried out, have made the process of fixing of accountability and subsequent prosecution extremely difficult. The shroud of anonymity behind which cyber-criminals operate has made the process of establishing the identity of transgressors anarduous one. Attribution is the first step in assigning responsibilities and seeking legal recourse against transgressors. If economic sanctions are used against Chinese firms accused of using U.S. trade secrets acquired through cybertheft, the Chinese reprisal will be quick and damning. The U.S. Chinese economic linkages grew steadily during the last decade and have become more interdependent and entwined;the commercial prudence does not justify such mutually incriminatorymeasures.On the other hand, it may adversely impact the mutually beneficial economic ties between the two counties as reprisals frequently lead to counter-reprisals and further escalation in already tense bilateral relations.

(Disclaimer: The views and opinions expressed in this article are those of the author and do not necessarily reflect the position of the Centre for Air Power Studies [CAPS])

Notes

[1]National Conference of Catholic Bishops, "The Harvest of Justice Is Sown in Peace: A Reflection of the National Conference of Bishops on the Tenth Anniversary of The Challenge to Peace" (Washington, DC: United States Catholic Conference, 1994).

[2] US Department of State, "Diplomacy in Action: Tran Sanctions", http://www.state.gov/e/eb/tfs/spi/iran/index.htm, accesses September 10, 2015.

[3] Somini Sengupta, "*U.N. Moves to Lift Iran Sanctions After Nuclear Deal, Setting Up a Clash in Congress", New York Times*, July 20, 2015, http://www.nytimes.com/2015/07/21/world/middleeast/security-council-following-iran-nuclear-pact-votes-to-lift-sanctions.html?_r=0, ,accesses September 10, 2015.

[4]David Nakamura, "U.S. developing sanctions against China over cyberthefts", *The Washington Post* , August 30, 2015, https://www.washingtonpost.com/world/national-security/administration-developing-sanctions-against-china-over-cyberespionage/2015/08/30/9b2910aa-480b-11e5-8ab4-c73967a143d3_story.html, accessed September 10, 2015.

[5] The White House : Office of the Press Secretary, "Executive Order -- "Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities", April 01, 2015,https://www.whitehouse.gov/the-press-office/2015/04/01/executive-order-blocking-property-certain-persons-engaging-significant-m, accessed September 10, 2015.

[6]Eric Holder, " Chinese military officials charged with stealing US data as tensions escalate", *The Guardian*, May 20, 2014, http://www.theguardian.com/technology/2014/may/19/us-chinese-military-officials-cyber-espionage, 20 May 14,accessed September 10, 2015.
