THE CENTRE FOR internet & society

Comments for the U.S. Department of Commerce

International Internet Policy Priorities

2nd July, 2018| Bengaluru, India

By **Swagam Dasgupta**
Edited by **Akriti Bopanna**

The Centre for Internet and Society, India

I. The Free Flow of Information and Jurisdiction

A. What are the challenges to the free flow of information online?

The Internet permeates throughout the globe yet its essential attributes such as data (and information) is seen as a regional concern. To put it another way, the Internet might be global but regulation is local. The free flow of information online faces the major challenge of data localization. Recently, many countries have sought to implement regulations requiring firms to store data on servers that are physically located within the boundaries of the nation. Given that this hinders the free flow of data across national borders, it is imperative to note that it emerges out of genuine concern and must not be easily dismissed. Data localization and the restriction of information have risen due to multiple factors.

First, the obvious vulnerability of personal information through cyber attacks, foreign government interventions and the use of user information for commercial purposes have proved to be critical issues for the free flow of data. Unless appropriate technical measures (such as homomorphic encryption) are taken to ensure and convince citizens of the safety of their data, this will always remain a barricade. Hence, it is not surprising that governments are seeking to assert physical control of data within their borders.

Second, information is political. Countries may attempt to block the flow of content that they believe to be morally objectionable. This could range from pornography, Nazi memorabilia sales online and the censoring of content inconsistent with their social beliefs such as gay rights, religious rights etc.[1] Censorship is also a seen as a matter of national security. As the internet becomes entangled within economic life, nations put themselves at the risk of cyber attacks from organized criminal networks, individuals and other governments. Coordinated efforts to from all nations to adhere to stronger international cyber law standards are crucial in order to mitigate the fear of information being used to undermine a nation's security.

Third, data localization is a form of economic protectionism. In order to boost the growth of domestic enterprises, governments are choosing to confine the relevant data within their borders. [2] Hence, foreign companies are inadvertently affected by this barrier to the free flow of information (data). Finally, the flow of information could be hindered in order to protect intellectual property rights. But, we must take into account that IP laws are an essential aspect of

[1] https://www.brookings.edu/wp-content/uploads/2016/06/internet-data-and-trade-meltzer.pdf

[2] https://www.albrightstonebridge.com/news/data-localization-challenge-global-commerce-and-free-flow-information

the economy. Hence, a balance must be maintained between the access to information online and IP rights of creators.

Therefore, the main challenge to the free flow of information online is the "fragmented patchwork of national jurisdictions" that is leading to a "legal arms race" on the internet.[3] More specifically, the internet undercuts traditional notions of national sovereignty, especially control over internal affairs. Increasingly, through the internet, multinational corporations and non-resident actors may influence a nation's public safety, political elections, and economic growth. "International cooperation" has proven inadequate to address these growing concerns. Unlike the technical specifications of the internet, competing laws and interests have prevented a cohesive international legal regime to govern "jurisdictional tensions such as cross-border access to user data, content takedowns, or domain seizures."

Additionally, the misuse of the free flow of information within and across national boundaries have increased tensions amongst citizens. As seen with the United States presidential election in 2016, misinformation arguably flows faster and farther than true information. Social media platforms excessively filtering content perhaps should not count as free flow. State actors may not be making these decisions, but the corporations that build internet architecture and platforms wield state-like power.[4] As a result, the negative consequences of the free flow of information are clouding its advantages. Without addressing concerns of misuse of data, governments will not only debate the flow of information outside and into its borders but might resort to restricting information flow within its territory.

The free flow of information has the potential to drive connection, innovation and productivity at a large scale. But, viewing this just through the lens of its advantages will only hold us back. Therefore, the priority of international organizations such as the IGF should involve discussions on maintaining a balance between the free flow of information and the necessary actions required to address the legitimate concerns of governments across the globe[5].

B. Which foreign laws and policies restrict the free flow of information online? What is the impact on U.S companies and users in general?

There are many laws and policies that restrict the free flow of information online. We will limit our answer to the case of India and China with regards to censorship and data localisation laws.

[3] https://www.internetjurisdiction.net/uploads/pdfs/Papers/IJ-Paper-Jurisdiction-on-the-Internet.pdf

[4] https://cyber.harvard.edu/works/lessig/pcforum.pdf

[5] https://www.brookings.edu/blog/up-front/2013/05/23/growing-the-global-internet-economy-by-ensuring-the-free-flow-of-data-across-borders/

Censorship

1.India:

Section 66A of the Information Technology, Act has been under fire for multiple cases since it criminalizes the practice of sending offensive messages using a computer resource. The wide scope and ambiguous wording allow it to be misused against users to shut down content and information that some might deem to be offensive, menacing, annoying and inconvenient. Although in relatively black and white cases such as the transmission of child pornography, such laws should be upheld, the ambiguity of the provision proves to be a barrier and inconvenience to the free flow of information online. Many times, this provision has been used in order to curb political dissent by both censoring the users content as well as in many cases, arresting the user (usually for a term of three years). Additionally, Section 69A authorizes the government to block any content from being accessed by the public on various grounds and any intermediary that fails comply can be sentenced to a prison term.

2. China:

In 2017, Chinese authorities enforced strict regulations on some of China's top streaming websites which included the removal of foreign TV shows. Additionally, online news websites are to be overseen by an editorial staff that is approved by the government, hereby, posing as a challenge to both the free flow of information online as well as the freedom of expression online. In order to access blocked websites, users have to go through numerous virtual proxy networks, but the 2017 regulations cracked down on the use of VPN's as well. Such a form of censorship of content from the level of the source harms the notion of a free and global internet for all.

Both India and China have censorship laws like much of the world, but they work to different extents. Users are the most affected as their freedom of expression is restricted (often unfairly) and through criminalization.

Data Localization:

1.India:

In 2012, India enacted a "National Data Sharing and Accessibility Policy," in which government data (data owned by government agencies or collected using public funds) are to be stored in local data centres. In February 2014, the Indian National Security Council proposed a policy requiring all email providers to set up local servers for their India operations and stated that all data related to communication between users in India have to remain within the country's jurisdiction. In 2014, India passed the Companies (Accounts) Rules law, requiring backups of financial information to be stored in India, if primarily stored overseas. 2015 saw India release a National Telecom Machine-to-Machine roadmap that requires all relevant gateways and application servers that serve customers in India to be located within India and data localization a requirement for cloud providers computing for public contracts.

2. China:

China has made several policy changes post the Snowden revelations. These restrict the cross-border transfer of data and a few are as follows:

a. In 2006, China initiated measures for e-banking that required such companies to keep their servers within China.
b. In 2013, China's new rules regarding credit reporting required all credit information on Chinese citizens to be processed and stored in China. Similar laws were applicable to health and medical information.
c. In 2016, Internet-based mapping companies would have to store their data locally as well.
d. In the same year, China enacted new regulations within cloud-computing services that essentially excluded foreign technology firms and reinforced local data-storage

The effects and reasons for data localization and censorship have been discussed in Question A. It is imperative to note that although these laws do pose a challenge to the free flow of information online to various extents, many of them are born out of legitimate concerns on data privacy, national security and domestic economy. We cannot dismiss the legitimacy of these regulations and demand free flow of information. International organizations and multistakeholder meetings must discuss these issues while taking into account the pluralism of each country (or even locally) in order to be an effective agent of change.

C. Have courts in other countries issued internet-related judgments that apply national laws to the global internet? What have the effects been on users?

The Internet's decentralised nature, low cost and quick speed allow it to be utilized as an effective catalyst for an interconnected global economy. But, this intricate global network of nations may lead to issues that involve parties from more than one national jurisdiction. The long reach of the internet makes it hard to examine the reach of national laws on the global internet. As far as we know, no single internet-related judgement has applied national laws to the global internet as a whole. But that's not to say that these laws do not affect other jurisdictions at all.

The extent, as well as the mode in which national laws affect the internet in other areas, vary according to the law. For example, Germany's sweeping law that subjects websites that are accessible to Germany to German law. As a result, the German government can hold ISP's guilty for violations of German content laws if they were aware of the content and able to remove it beforehand.[6] In such a system, any user from outside and inside Germany that promotes Nazi or neo-nazi viewpoints will not be able to share the objectionable content within the German jurisdiction. Therefore, the effect of this law extends to the subset of people who wish to share that content as well, but not necessarily to the entire global internet. Similarly, Malaysia's cyberspace law extends well beyond the borders of Malaysia. It applies to the offences committed by a person within or outside of Malaysia, "if at the relevant time the computer, program, or data was either (i) in Malaysia or (ii) capable of being connected to or sent to or used by or with a computer in Malaysia. The offender is liable regardless of his nationality or citizenship."[7]

Multiple businesses outside the EU have realised the extraterritorial nature of the GDPR regulations. Even if a company has no direct EU operations, it may still need to comply, arguably as long as they're processing information of individuals in Europe. Even large companies within the US, such as Facebook, have changed their privacy policies to cover topics present in the GDPR. As a result, EU's GDPR regulations have changed the way many (but not all) online businesses outside the EU conduct their operations. In 2014, the European court ruled in favour of a Spanish citizen who filed a case against Google for displaying an archived newspaper item that consisted of details regarding his past. The court asked Google to "delist" said article from the search engine. This came to be known as the right to be forgotten and has seen citizens of other countries demanding the very same right from Google.

The fact that the GDPR data protection law is based on a set of clearly-structured instruments makes it attractive to other countries. As a result, the EU law reaches over to other jurisdictions indirectly as other countries might find it easier to apply the basic framework of the GDPR to their jurisdiction rather than drafting a new one from scratch.

Overall, the effects of the extended reach of national laws have affected users in different ways. The GDPR has brought power to the user by giving them the right to know what information is being collected as well as the right to be forgotten. In contrast, laws such as that of Germany (discussed above) do not allow for the free flow of information and acts as a restriction to the freedom of expression. Each law affects users within and outside the law's jurisdiction differently and hence, must be dealt with separately.

D. What are the challenges to freedom of expression online?

[6] https://cyber.harvard.edu/property99/domain/Betsy.html
[7] https://cyber.harvard.edu/property99/domain/Betsy.html

Although the Internet is an avenue that promotes connection, innovation, productivity and should support the right to hold and express one's opinion, there currently exist multiple barriers to the freedom of expression online.

First, many countries officially and unofficially employ methods to deny citizens the right to access documents held by public bodies. This poses a direct threat to democratic participation and hinders the intervention of both the media and civil societies. Therefore, legislative transparency should be a policy measure and enforced effectively.

Second, the liability of internet intermediaries (such as ISP's) online has the potential to restrict the freedom of expression. Privatized policing through coercion or public relations pressure results either in the content being removed from the platform or lawsuits. The obligations imposed on the intermediaries should not lead to unintended yet dangerous restrictions on the freedom of expression. The Manila Principles on Intermediary Liability are a good guideline to avoid this problem and chart a legally flexible intermediary regime that does not unduly compromise these content holders/sharers.

Third, expressing one’s views on popular social media websites could incur significant backlash. Publicly expressing a differing or extreme political view, for example, have led to arrests on the basis of sedition as well as death threats from non-state actors in many countries. Usually, these incidences are based on the political, religious and cultural climate of the country. Hence, coercion by the state or others could also curb freedom of expression online. Countries should enforce laws in accordance with international human rights laws in order to prevent the suppression of opinion unless for legitimate reasons such as sharing child pornography etc.

Fourth, the threat to net neutrality represents a valid concern that is proving to be hard to combat. The freedom to access the internet cannot exceed the freedom the view any page without bandwidth throttling, resulting in the access to only a particular set of web pages. Any person should have the right to view what they wish to see except in unacceptable cases.

The digital world has seen content being controlled by the same technologies that delivered it — servers that allow us to access the network could be utilized by bodies to block certain websites, ISP’s can be used to deny access to websites that have particular keywords (on the orders of various state and non-state actors), text messages can be intercepted in order to track protestors, censorship software can be built into systems to deny access to parts of the internet in such a way that the user is not aware of it, search engines can deny access to certain web pages and can, in turn, send the user to “safe” and “controlled” web pages etc. Additionally, the monitoring of online content by law enforcement and malicious users, coupled with arrests of ‘cyber-dissidents’ create a dangerous environment wherein the safety of citizens is not enforced, although guaranteed in theory. All stakeholders from around the globe need to take into account the plurality of each nation and find a way to enforce strict adherence to international laws regarding freedom of speech and expression online. They need to address the lagging legal frameworks as well as the lack of access to the internet in such a way that freedom of expression remains a priority.

E. What should be the role of all stakeholders globally—governments, companies, technical experts, civil society and end users — in ensuring free expression online?

Our reply to question F. depicts the importance of all stakeholders in the matter of securing freedom of expression online. Amongst the five given stakeholders, governments should discuss their own definition and boundaries to the freedom of expression. This will prove to be extremely vital because of the cultural, religious and social differences between each nation. The definition of dissent itself will vary considerably. Hence, a non-confrontational atmosphere to discuss these limits should be made available. The private sector should also take part in this conversation since they are arguably the next or equal in power with regards to regulatory capacity when compared to governments. It is imperative that the legalities with respect to the private sector, including internet intermediaries are discussed. The technical experts should present standards that are designed to protect the freedom of expression and must try to convince the private sector to utilize it. Finally, civil societies must play the voice of reason and diversity, advocating for the groups that have been punished unfairly. Governments and private sector firms should consult all the stakeholders and decide upon international rights and how they are to enforce it as well as the standards they would choose to make sure that freedom of expression is not taken away from the end user.

F. What role can NTIA play in helping to reduce restrictions on the free flow of information over the internet and ensuring free expression online?

NTIA could advocate for governments to adhere to international standards of freedom of expression online in international multistakeholder forums/organizations such as the IGF and ICANN. They, along with all other stakeholders must play a vital role in establishing an international code for expression online. Additionally, NTIA could work with other stakeholders to address the legitimate concerns of nations in order to reduce data protectionism. For example, by lobbying for better cyber policies on a global scale, the threat of cyberattacks on nations should not be enough of a problem to invoke data protectionism. In the same manner, NTIA should aim to solve the fundamental issue with the free flow of information in order to convince the world of its advantages. For example, new avenues to curb widespread fake news could be discussed within international forums.

G. In which international organizations or venues might NTIA most effectively advocate for the free flow of information and freedom of expression? What specific actions should NTIA and the U.S. Government take?

The issues of the free flow of information and freedom of expression should be discussed in multilateral, regional, bilateral forum and multistakeholder forums. Since the trading of data is rapidly increasing in pace and volume, resulting in increasing economic gains, the issue of the free flow of information must be discussed within the WTO. Freedom of expression must be debated locally and internationally. Since this necessarily requires international humans rights laws, there must be extensive debates in a multistakeholder environment including governments, the private sector and most importantly, civil societies. Other bodies such as UNESCO could take an active part in the negotiations as well. NTIA should aim to play a pivotal role within the IGF and ICANN with respect to who can or cannot hold domain names and to establish a set of norms that could be held as an international standard.

II. Multistakeholder Approach to Internet Governance

A. Does the multistakeholder approach continue to support an environment for the internet to grow and thrive? If so, why? If not, why not?

Internet governance consists of a set of multidisciplinary processes -- participation of governments, private sectors, civil societies and technical and academic communities. The discussions include the internet's technical, social and economic consequences as well as the development of shared principles, standards and decision-making procedures. Hence, there is an explicit need for multiple stakeholders to be involved in both the discussion and implementation processes of internet governance. The multistakeholder approach successfully includes diverse strata of society to create an inclusive environment for decision making.

Although in theory, the multistakeholder approach should support an environment for the internet to grow and thrive, in practice, it does not seem to do so. The two major factors that drive multistakeholderism are diversity and consensus amongst stakeholders. Although these are noble intentions, diversity and consensus often find themselves to be opposing forces. It is imperative to understand that diversity cannot exist for the sake of itself. Diversity is only useful insofar as it brings a different policy ask to the table. Consensus is useful only if it will result in effective self-regulation. In order to achieve both diversity and consensus, the IGF cannot view them as general attributes of all stakeholders. That is because each stakeholder represents a different community and differs in terms of their regulatory power. Not taking the heterogeneity of the stakeholders in account leads to the false premise that everyone in the IGF has an equal footing and shares the same aim. It is important to note that consensus should be sought out in the private sector while diversity should be sought out within civil societies.

Our recommendations to alter the IGF structure in order to reflect the heterogeneity of the stakeholders is given as a response to question H.

B. Are there public policy areas in which the multistakeholder approach works best? If yes, what are those areas and why? Are there areas in which the multistakeholder approach does not work effectively? If there are, what are those areas and why?

The multistakeholder approach has been implemented in the field of the internet, environment and food safety governance. The inclusion of multiple stakeholders from various disciplines promises diverse dialogue from each section of society. Hence, it serves as a good initial step towards decision making and problem-solving via inclusivity. But, there lies a fundamental problem with the method of operation within the present multistakeholder models — the failure to recognize or acknowledge the asymmetries of powers amongst stakeholders. By taking into account the differences in power, multistakeholderism could prove to be an effective model of governance aimed at consultative self-regulation.

Food Security Example:
Between 2013 and 2014, members from civil societies engaged in conversation to draft global guidelines to governments and the private sector to increase their Responsible Agricultural Investment (RAI). These consisted of meeting organized at the Food and Agriculture Organization's Committee on World Food Security (CFS) in Rome. Yet, after much deliberation, the final draft reflected a model that supported foreign investment that threatened the right to food for the most vulnerable populations. This was a result of asymmetries of powers amongst stakeholders[8].

The failure to recognize and act against the differences in stakeholder capacity lowers the extent of effectiveness of the multistakeholder system. We cannot say for certain that it has worked better in one case, mainly because there are no well-defined metrics that allow us to gauge this concern. Although consensus could be used to measure the effectiveness of the approach, the food security example cited above depicts how the coercive capacities of powerful stakeholders could distort the use of consensus as a metric. Therefore, formulating a metric to examine the effectiveness of the multistakeholder system across different use cases should be a priority.

[8] http://asiapacific.anu.edu.au/regarding-rights/2015/05/22/negotiating-rights-multi-stakeholder-governance-global-food-security-and-the-right-to-food/

D. Should the IANA Stewardship Transition be unwound? If yes, why and how? If not, why not?

The IANA Stewardship Transition should not be unwound. The transition has significantly improved ICANN's accountability with the global multistakeholder body coming up with more almost 100 recommendations to do so. Additionally, reverting it to the NTIA is strongly against the notion of global internet freedom. This is because internet protocols are not just used in the United States, but globally. Hence, the domain of internet governance itself is a global concern and must involve the participation of actors from all over the world. Post the transition, multiple stakeholders hold claim to discussions on internet governance. This includes the private sector and civil societies to name a few. It marked a paradigm shift towards private governance as opposed to intergovernmental or merely governmental governance. A reversal of the IANA transition could send the signal that the United States wants the government to be in charge of the Internet. This can have dire consequences as other governments might not hesitate to assert their respective claims. If this is the case, internet governance might find itself amongst the tension of geopolitics. A structure in which multiple stakeholders — including bodies other than governments and the private sector — have the ability to consult one another must be maintained for a free and open internet.

E. What should be NTIA's priorities within ICANN and the GAC?

As a representative of the United States government in ICANN's Governmental Advisory Committee (GAC), NTIA should work with other governmental and intergovernmental bodies, and priorities three key activities:

1. The inclusion of stakeholders other than the existing members in order to improve consultation.
2. Maintain the accountability and transparency in its practices.
3. Protection from cybersecurity threats, including the capacity to prevent the misuse of Internet unique identifiers etc.

G. Are there barriers to engagement at the IGF? If so, how can we lower these barriers?

Yes, there exist multiple barriers to engagement at the IGF. A major issue stems from the fact that the multistakeholder model wrongly assumes that each stakeholder has an equal footing in the process and resultantly, outcome. It does not take into account the relative regulatory power of each entity. In order to understand the unequal distribution of power, the following questions should be used to examine the strengths of four major stakeholders (Governments, Private Sector, Technical and Academic Community and Civil Societies):

1. Does the stakeholder/entity have the capacity to govern?
2. Does the stakeholder/entity have the capacity to govern itself, i.e, self-regulation?
3. Who is being governed?
4. How is the stakeholder/entity governing or regulating?

a. Government: Governments have the capacity to govern **almost all** other stakeholders. This is usually done by producing and enforcing national laws within a given jurisdiction. Governments are also free to pass laws that regulate itself and can, therefore, self-regulate. For example, the Indian Government regulates itself through the Right To Information (RTI) Act.
b. Private Sector: The private sector can also regulate **almost all** stakeholders by utilizing the power of the market. For example, because Facebook has a monopoly within a particular social media market, they could make sure that something is done relatively faster than government entities. The private sector has the capacity to self-regulate, but they may not always choose to do so.
c. Technical and Academic Community: This community has the capacity to govern **indirectly** by producing certain standards. For example, a government or private sector cannot break our Whatsapp communication because of the standards used in the application. The technical and academic communities cannot self-regulate as there exists no clear-cut method to make sure they restrict their behaviour.
d. Civil Societies: They can **influence t**he government and private sector by organising protests etc., but they do not have the genuine capacity to regulate other stakeholders. Their powers of influence are demonstrated rarely and they **cannot** practice self-regulation.

By analysing the multistakeholder model through this framework, it is obvious that there exists a hierarchy due to differences in relative regulatory capacity at the IGF. Governments and the Private sector enjoy a more powerful position when compared to the Technical and Academic community and Civil Societies. These differences need to be reflected in the procedure of the IGF through a change in structure in order to increase the impact of stakeholder engagement.

Additional reasons are as follows:

1. Conceptually, the role of each stakeholder is still ambiguous. The notion of multistakeholderism itself is not clearly laid out anywhere, which results in an ambiguity in understanding the role of a stakeholder in the system.
2. In many countries, civil societies are often in their nascent stages and therefore, incapable of performing their respective role. This results in an imbalance of forces amongst stakeholders in the IGF, often in the form of less engagement and abandonment by the civil societies.

3. Relatively low participation of stakeholders from developing countries since the agenda is rarely on problems that they are currently facing. Many stakeholders that do not have access to the necessary education and training for discussions on Global Internet Governance.
4. Lack of resources amongst stakeholders in developing countries to actively attend discussions on global Internet governance issues.
5. Openness and transparency in the management of critical resources and functioning of the IGF and other bodies.
6. Time constraints usually impede and disrupt constructive discussions. Additionally, some topics require more time for a better and deeper understanding. The current format of the IGF ignores this issue.
7. There exists no global consensus on the extent of the role of Governments within Internet governance.
8. Transparency with regards to agenda setting is unclear. For example, the following workshop proposal topics were rejected : "roles of the Internet in anti-poverty strategies" and "regulating global Internet businesses - need for global frameworks" for the 2013 IGF.
9. Finally, the existing model of multistakeholderism does not take into account the capacities and roles of different stakeholders well enough.

H. Are there improvements that can be made to the IGF's structure?

The structure of the IGF could be altered to reflect the differences in regulatory capacity amongst stakeholders. We recommend the following structure:

1. In general, the IGF discussions should prioritise learning about global internet governance within a non-confrontational space.
2. For the first two days, each stakeholder group should gather and create sub-communities amongst themselves.
    a. Industries and firms within the private sector could form sub-communities based on having similar stances on labour laws or net neutrality laws. Additionally, firms that believe that they have the capacity to self-regulate should form a sub-community and come up with their own self-regulating norm.
    b. Similarly, if a group of governments agree that a particular set of areas within the private sector require regulation, they should for a sub-community. Furthermore, the governments within the sub-community should the discuss how they could cooperate with one another to roll out the regulation.
    c. The technical and academic organisations should create sub-communities based on which standards they believe are essential to prioritise and present to other stakeholders.

    d. Unlike the other stakeholders, civil societies should not focus on consensus. Instead, they should identify how they differ from one another. The civil societies should arrange themselves in a continuum of differences.
3. For the following days, the proceedings could be as follows:
    a. The private sector sub-communities will present their plans on self-regulation to all other stakeholders.
    b. Similarly, the sub-communities of governments will present their plans and justifications for regulation to all other stakeholders.
    c. The technical and academic sub-communities should recommend standards that they believe should be adopted.
    d. The civil societies should provide feedback to the bodies with the regulatory power (governments and private sector).
4. Repeating this process of consultation amongst the stakeholders (a. to e.) will lead to consensus regarding a particular regulation.
5. In this way, the multistakeholder model is made to focus on **consultive self-regulation** at the IGF, such that each stakeholder is at least consulted before any regulation goes through. In this way, governments and the private sector are aware of the number of civil societies that support their regulation as well as the number of technical bodies that support their standard. They can choose to alter their regulation in order to garner more support from other stakeholders. No group is tied down by another, instead, any group is free to act as long as they amass enough support.
6. Therefore, by taking into account the plurality of the stakeholders with respect to their regulatory powers, this structure promotes consultive self-regulation and hence, consensus.

III. Privacy and Security

A. In what ways are cybersecurity threats harming international commerce? In what ways are the responses to those threats harming international commerce?

The internet has allowed businesses to sell products and services while engaging with customers in a cost-effective, yet personal manner, giving rise to E-commerce in its present form. Trade across national borders through the internet has gotten almost every country connected to one another. Hence, unless global efforts are made to enhance the security of international and local trade online, there could be dire consequences on the world's economy. E-commerce websites are prone to numerous types of cyber attacks that affect firms in different ways.[9] In fact, this huge growth in the popularity of e-commerce firms has led to a harmful generation of

[9] http://serialsjournals.com/serialjournalmanager/pdf/1500284389.pdf

personalized cyber attacks. Hence each website must have the following security features at least:

1. Means to authenticate identities correctly (for secure transactions).
2. Integrity of messages - messages cannot be modified between while in transition.
3. Non-repudiation: Sender of that message cannot deny sending it.
4. Effective access control systems
5. Availability of necessary resource to authorized personnel at all times.

The most common threats to E-commerce websites can be categorized as follows:

1. **Fraud**
   Financial records can be transferred from one account to another or deleted completely. Criminals can use malware to manipulate insecure transactions and steal vital bank account information. These could lead to liabilities and major losses for e-commerce websites. A few examples are:
   a. Identity fraud: Criminals can forge someone's existing identity to make "card not present" transactions online. Additionally, they can order items online using aliases or by using someone else's account. Usually, all they need is a stolen password. Hence, e-commerce websites could incur massive financial costs due to identity fraud.
   b. Friendly fraud: E-commerce organizations can face losses if customers order goods or services using their debit or credit card. Furthermore, they claim that their account details were stolen and demand a refund.
   c. Clean fraud: Stolen credit card information is used to make payments. Furthermore, their transaction is manipulated to bypass the fraud detection mechanism completely.
   d. Affiliate fraud
   e. Triangulation fraud
   f. Merchant fraud: A fake online store offers items at extremely low prices but never ships them. Instead, the payment is kept by the fake store. This could also take place at the wholesale level and disorient the working of retail e-commerce sites.

2. **Phishing**
   Phishing attacks can also lead to financial losses to e-commerce organizations as well as lower their reputation with regards to the safety of their users.
   a. Trojan horses are installed on machines to collect vital information.
   b. Hackers distribute generated login details to cyber criminals.
   c. Certain softwares prevent users from not being able to download malicious code.

    d. Common methods are: link manipulation, graphical substitution, DNS cache poisoning, filter evasion.

3. **Server Threats**
   The client-internet-server trio is essential to bridge the path between e-commerce servers and users. But, servers are also a point of vulnerability that can be misused and result in the illegal distribution of information, losses and other liabilities.
    a. Hacking directly into the e-commerce organizations database to steal, manipulate or delete private information.
    b. Web server threats
    c. Common Gateway Interface Threat

4. **Password hacking**:
   The effect of which have already been discussed above.

5. **Pharming**
   Targets DNS systems and affects the internet routing system by intervening with the lookup process of the domain name. So a customer search for ebay.in could be taken to a similar looking site unknowingly leading to losses for ebay.

In general, e-commerce organization can be heavily affected by cyber attacks in the following ways:

1. Direct financial loss due to fraud: Additionally, many companies think it’s easier to pay the hackers for their data which leads to a vicious cycle that repeats on end.
2. Loss of consumer confidence and in turn, market share
3. Criminal charges due to the breach of regulatory requirements
4. Brand is affected
5. Loss of productivity