Problem 1

Collaboration Statement: My work on this problem is completely independent and I did not collaborate with any students or external sources.

a) SEQ: $B + 1 + L_2$
ACK: $A + 1 + L_1 + L_4$
Src: P_S
Dst: P_C
b) (i) Raj can observe a packet, and note its SEQ and ACK. Suppose this packet has length L_1, $SEQ = A$ and $ACK = B$. He can then send a packet in the opposite direction with length L_2, $SEQ = +1$, and $ACK = A + L_1$. If this is sent at the the same time and in the same direction as a packet with length $L_3! = L_2$, and Raj's packet is received first, then the actual packet will be discarded as its SEQ and ACK are invalid, allowing Raj to hijack the connection and his packet will be accepted first. This is hijacking the connection, as he can do this in either direction and his packets will be accepted in place of real packets.

(ii) Kaki can make the same attack happen, but she has no idea what the starting SEQ and ACK are. So, she should send as many packets as she can, with as many different SEQ and ACK combinations as she can, in hopes that one of them will be accepted in the same way that Raj's were.

c) In RSA Key exchange, a key R is encrypted by the web browser using a public key PK_R, and $C = E_PK(R)$ is send to the web server. From there, the server computes $R = D_SK(C)$. Forward secrecy is the guarantee that the compromise of public-key encryption private keys does not break confidentiality of past encrypted messages. An attacker can eavesdrop on TLS communication and store all communications. If the SK is compromised, then the attacker can simply recover the secret key by decrypting that specific message. Thus, TLS with RSA key exchange does not provide forward secrecy.

Problem 2

Collaboration Statement: My work on this problem is completely independent and I did not collaborate with any students or external sources.

a) $[1, E(PK_1, [2, E(PK_2, [8, E(PK_8, [9, E(PK_9, [4, E(PK_4, [10, E(PK_{10}, M))))))]$

b) The confidentiality of M is not maintained. This is because of the last hop (node 10 to node 11) in which the message M is not encrypted (because each of the encryption layers in part (a) have been decrypted). So, an adversary can simply eavesdrop on this last step of the connection and read M).

c) Yes, this is possible. When a packet is sent, Sierra can save the packet that is sent from the router to the first node in the TOR network, and she can also monitor the traffic that travels from the last node the gradescope, which she can save as well. If she takes a packet that was leaving a computer and resends it. She then starts a timer, and stops a timer when a packet reaches gradescope which is identical to one she's seen before. Using this knowledge, she can find the wire distance that a packet travels, and can use that to associate handins from that particular user with their computer which it was originally sent from (since each wire distance is unique).

d) Yes, it is possible. She can monitor traffic leaving your computer, and can monitor traffic reaching gradescope. Since you're the only one sending traffic, only one handin reaches gradescope so she knows when you've sent a packet and that it's yours. This is why it's important that multiple people use a Tor network in order to guarantee privacy!

Problem 3

Collaboration Statement: My work on this problem is completely independent and I did not collaborate with any students or external sources.

a) The US should threaten economic sanctions to any state guilty of committing, funding, or otherwise supporting cyberattacks against critical US targets (electrical grids, transportation, etc). This needs a very high confidence in attribution; although cybercrimes are sometimes difficult to track down and there is no ”clear and convincing standard” for attribution, the U.S. should establish clear and consistent metrics for any case of retribution. Ideally, these would be debated on and determined by Congress, since it’s important that the U.S. doesn’t sanction countries that did not commit cybercrime.

b) One barrier for international law is the lack of ”clearly defined terms”, which includes phrases such as ”internationally wrongful act”, which do not have a meaningful legal definition, and thus are impossible for international governing bodies to utilize when responding to cyberattacks. Another barrier is that it is difficult for international bodies to regular nonstate actors, which are a major factor in committing cybercrime. Finally, many states ”have chosen not to subject themselves to international standards”, because the benefits of cooperating with such a system are outweighed by the political or economic gains that can be made by refusing it. Overall, I agree with the author that it is difficult for international law to regulate cyberattacks. In order for these problems to change, many countries would have to agree to work towards standards of cybersecurity, and this sort of cooperation seems unlikely. Additionally, even if those standards did exist, problems with non-state actors would not go away, making cybersecurity regulation even more difficult.

c) I think that it would be better for governments to take this active role in shaping cyberspace norms. While many of the goals of these non-state actors are good, they are also not democratically elected nor are they accountable to anyone except their shareholders. Ideally, governments that are democratically elected can shape these norms, since they are more likely to have the interests of the people at heart.