Sandworm Reading Schedule and Discussion Guide

"Couched within the fascinating journeys of real-world characters striving to understand the implications of our evolving cyber world, no other book provides as rich and accessible a discussion of cybersecurity, threat intelligence, critical infrastructure, and nation-state threat actors as Greenberg's *Sandworm*."

-Sean McBride-

Meeting	**Chapters**	**Study** Come prepared to discuss these questions on the meeting date
Week 1		
Week 2	Intro & Prologue	• What does Greenberg describe as the significance of Ukraine attack? • What made the books first character suspect the event was caused by a cyber attack?
Week 3	1-3	• What type of firm was iSIGHT Partners? • Identify and briefly describe three roles that existed within the company. Provide the names of one individual per role. • What technique did the malicious attachment use to convince the recipient to open it? • What lucky finds provided significant clues about the malware? • What did the researcher suspect could be a type of crime scene fingerprint? • What is virus total? • What challenge did the firm face in going public with their findings?
Week 4	4-6	• What other firm and researchers also worked on the trail of these compromises? • What linked sandworm to industrial control systems? • What experiences prepared Hultquist for his current role? • Why do you think the author does not provide any description of how the DHS ICS-CERT obtained information about other control Systems vendors linked to the campaign? • Why is the compromise of a domain controller important? • What things piqued Yasinski's interest in the technical world? • Name and briefly describe several significant events in Ukraine's geopolitical history
Week 5	7-9	• Why are the media enticing targets for nation-states? • What did the Ukrainian president believe were the aims of the cyber and kinetic attacks? • To what extent do you agree with President Ushenko's remarks that the Bell tolls for all of us?

		• Regarding iSIGHT's prediction of a blackout, what would you have done if you were a US utility and received this warning? • What do you think about the US government's hesitancy related to revealing black out details? • What technique caused the blackout?
Week 6	10-12	• What made Assante's background unique? • Describe a key take away from the Aurora test. • What was Kevin Mandia's claim to fame? • Identify several key cybersecurity developments displaying the development of Russian cyber capabilities. • What is the fog of war, and how did it apply to the president of Estonia? • How did the techniques used against Estonia evolve? What may have been the logic behind this evolution? • What explanation does the author give for NATO members to not invoke article 4 and 5?
Week 7	13-15	• How did Arbor track DDOS botnets? • What was new about the use of cyber in the republic of Georgia? • What was the purported third option for President Bush related to Iran? • How would you approach troubleshooting failing centrifuges? • Do you spot any inconsistencies in the way the author tells the Stuxnet story? • How does Stuxnet compare with previous cyberattacks? • Why did Rob Lee make the blog post and not Mike Assante? • Was the US government's response appropriate? Why or why not?
Week 8	16-18	• Were Fancy Bears’ activities ultimately effective? Why or why not? • What is the technical name the analyst give to Fancy Bears activities? • What tools and techniques allowed Matonis to spot interesting malware? • What's new obfuscation techniques have the attackers used? • What were some of the key differences between the 2015 and 2016 blackouts in Ukraine? • What was the name of the application that provided access from the business side of a network to the industrial side of the network? • Describe several theories that explained why large State actors would or would not use cyber attack on critical infrastructure
Week 9	19-21	• What did Cherapanov do to get hired at ESET? What advantage did his firm have and identifying new malware? • Do you think Rob Lee's actions in creating a report about in destroyer we're ethical? Why or why not?

		• In what way were the commands sent by Industroyer indistinguishable from legitimate commands? In what way were they distinguishable? • Who in the United States has the define mission of providing early warning of cyberattacks against the electric grid? • What made the Siprotec vulnerability so concerning? • Would you be nervous to go to work for a federal agency that engaged in offensive operations? Why or why not? • Why is patch management so difficult? • Explain the deep irony of the Shadow brokers release of eternal blue.
Week 10	22-26	• What was Hutchins clever idea? Would you have thought of this? Why or why not? • What hypotheses would explain why Microsoft respond this way to the Mimikatz flaw? • Why are update servers high value targets?
Week 11	27-30	• What is the difference between a hot site and a cold side? What are the disadvantages of a hot site? is there any analogy in industrial control world? • What would you say is the underlying reason for the effects achieved by Notpetya? • What do you think is the value information sharing organizations like the healthcare cyber task force? • Do you believe the hospital reports that no dangerous procedures were carried out? Why or why not? • Why is early warning so difficult to achieve? • Greenberg claims that Sandworm is Telebots. Do you believe him? • Why didn't the Intellect Service CEO (Linnik) think her firm would be a target?
Week 12	31-33	• Describe the culture that the GRU established to discourage turn coats. • Do you agree with Greenberg's assertion that GRU cyber operators are insidious? • Was the White House response convincing to you? • Does Greenberg convince you that there's another group, apart from Sandworm, that has critical infrastructure hacking capabilities? •
Week 13	34-36	• What is a watering hole? • What lessons do you learn from the Korean Olympics attacks? • Do you agree the attribution of cyber-attacks is hard? • Describe Matonis big discovery. • Why was Matonis laughing when he made the discovery?
Week 14	37-39	Why was the Greenberg surprised at the FireEye web of analysis?

		Do you think the individuals in the indictments are bad people? Why or why not? Why is attribution so difficult? Why is attribution so easy? Why is it important to recognize how adversaries are structured? Why do government communications only provide conclusions rather than actual evidence? What are the pros and cons of that approach? In intelligence speak what do terms like "highly confident" mean? Should analysts mix special terms such as "highly confident" with other descriptors like "almost certainly" in a single sentence? Why or why not? Why does Greenberg end up putting so much confidence in the UK report? Was Hultquist's epiphany an epiphany to you? Why or why not?
Week 15	40 - Appendix	Summarize the offense vs defense argument. Do you think a cyber Geneva convention is possible? What does Dan gear mean by "Rubicon"? What can you do to increase recoverability at the places you work?
	Reflection	Identify three key ideas in the book and provide two examples from the text to support each. Is the United States paying enough attention? Why or why not? Assuming that you were running a cybersecurity team at a large US utility, and you could only afford to purchase intelligence from Dragos (represented by the philosophy of Rob Lee) or intelligence from FireEye (represented by the philosophy of John Hultquist) which service would you purchase? Why?