# Reading Assignment—Sandworm

Please read Sandworm by Andy Greenberg. I encourage you to read the entire book, but you can get what we need for this class by reading these chapters:

1-5, 8, 9, 15, 17-19, 20 – 29

There are several threads in this book, and here are some of them:

* Attacks against the Ukraine power grid and digital infrastructure
* Work by Software Reverse Engineers (SRE) around the world to understand the attacks
* The NotPetya attack on Ukraine and companies that did business in Ukraine
* Supply chain attacks: an attacker that compromises a software company can easily distribute its malware to the company’s clients
* History of the conflict between Russia and Ukraine
* Attributing the attacks to Russia, and determining which Russian government agencies are responsible
* US politics related to the attacks against Ukraine

For this class, we are only interested in the top three bullets, with an emphasis on the effort to defend against malware attacks. If you are reading something that does not apply to reverse engineering malware or malware attacks, feel free to skip ahead.

As you read, jot down notes on things that are:

* Especially relevant to this class
* Interesting or amusing
* Anything else you’d like to bring to the attention of our class.

Please hand in either ½ to 1 page about your notes, or 8-10 bullet points about your notes. This is not a book report! Instead, it is a list of your observations about interesting or IT security related items you found in the book.