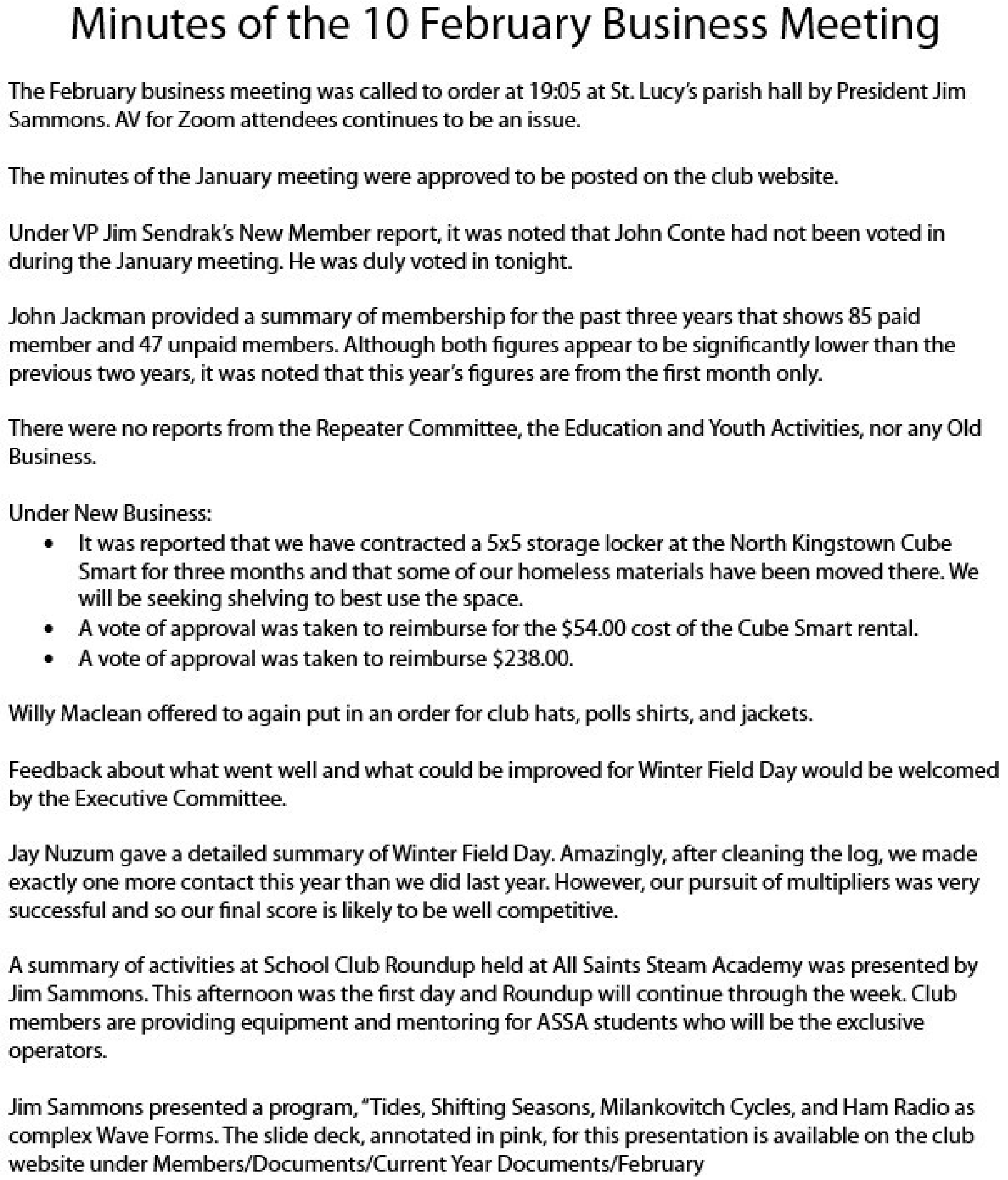
75

NEWPORT COUNTY RADIO CLUB

75

March 10, 2025



Minutes of the 10 February Business Meeting

The February business meeting was called to order at 19:05 at St. Lucy's parish hall by President Jim Sammons. AV for Zoom attendees continues to be an issue.

The minutes of the January meeting were approved to be posted on the club website.

Under VP Jim Sendrak's New Member report, it was noted that John Conte had not been voted in during the January meeting. He was duly voted in tonight.

John Jackman provided a summary of membership for the past three years that shows 85 paid member and 47 unpaid members. Although both figures appear to be significantly lower than the previous two years, it was noted that this year's figures are from the first month only.

There were no reports from the Repeater Committee, the Education and Youth Activities, nor any Old Business.

Under New Business:

- It was reported that we have contracted a 5x5 storage locker at the North Kingstown Cube Smart for three months and that some of our homeless materials have been moved there. We will be seeking shelving to best use the space.
- A vote of approval was taken to reimburse for the $54.00 cost of the Cube Smart rental.
- A vote of approval was taken to reimburse $238.00.

Willy Maclean offered to again put in an order for club hats, polls shirts, and jackets.

Feedback about what went well and what could be improved for Winter Field Day would be welcomed by the Executive Committee.

Jay Nuzum gave a detailed summary of Winter Field Day. Amazingly, after cleaning the log, we made exactly one more contact this year than we did last year. However, our pursuit of multipliers was very successful and so our final score is likely to be well competitive.

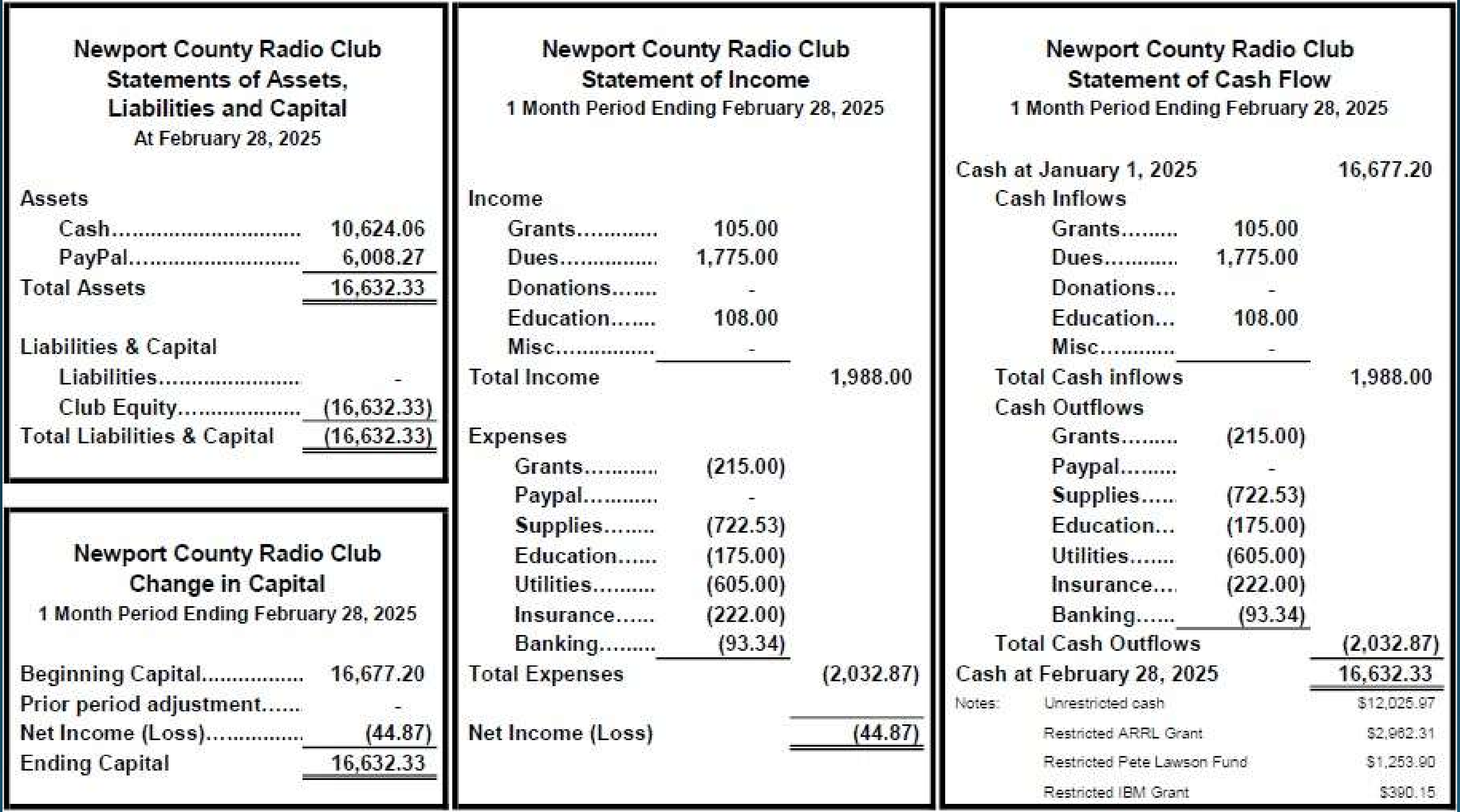
A summary of activities at School Club Roundup held at All Saints Steam Academy was presented by Jim Sammons. This afternoon was the first day and Roundup will continue through the week. Club members are providing equipment and mentoring for ASSA students who will be the exclusive operators.

Jim Sammons presented a program, "Tides, Shifting Seasons, Milankovitch Cycles, and Ham Radio as complex Wave Forms. The slide deck, annotated in pink, for this presentation is available on the club website under Members/Documents/Current Year Documents/February

New Members

Report from Vice
President
Jim Sendrak, KC1LYG

Treasurer’s Report, February 2025



Newport County Radio Club
Statements of Assets, Liabilities and Capital
At February 28, 2025

Assets	
Cash..............................	10,624.06
PayPal...........................	6,008.27
Total Assets	16,632.33
Liabilities & Capital	
Liabilities.......................	-
Club Equity....................	(16,632.33)
Total Liabilities & Capital	(16,632.33)

Newport County Radio Club
Change in Capital
1 Month Period Ending February 28, 2025

Beginning Capital.................	16,677.20
Prior period adjustment......	-
Net Income (Loss)................	(44.87)
Ending Capital	16,632.33

Newport County Radio Club
Statement of Income
1 Month Period Ending February 28, 2025

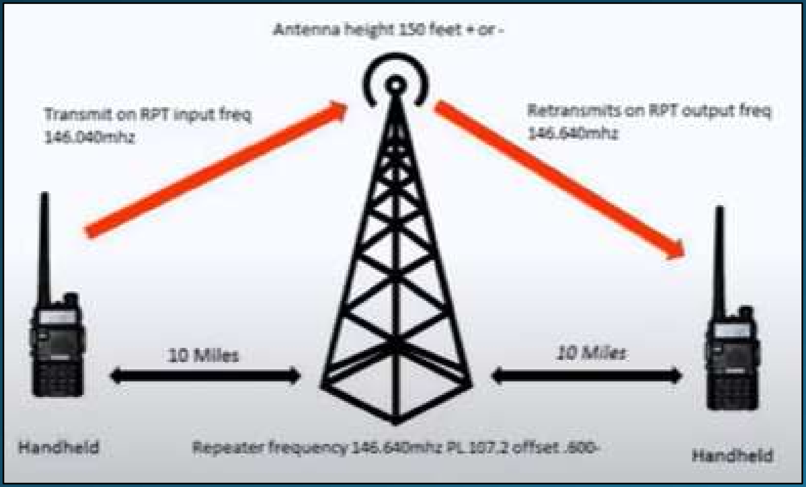
Income		
Grants............	105.00	
Dues...............	1,775.00	
Donations.......	-	
Education.......	108.00	
Misc...............	-	
Total Income		1,988.00
Expenses		
Grants...........	(215.00)	
Paypal...........	-	
Supplies........	(722.53)	
Education......	(175.00)	
Utilities..........	(605.00)	
Insurance......	(222.00)	
Banking.........	(93.34)	
Total Expenses		(2,032.87)
Net Income (Loss)		(44.87)

Newport County Radio Club
Statement of Cash Flow
1 Month Period Ending February 28, 2025

Cash at January 1, 2025		16,677.20
Cash Inflows		
Grants.........	105.00	
Dues...........	1,775.00	
Donations...	-	
Education...	108.00	
Misc...........	-	
Total Cash inflows		1,988.00
Cash Outflows		
Grants.........	(215.00)	
Paypal.........	-	
Supplies.....	(722.53)	
Education...	(175.00)	
Utilities.......	(605.00)	
Insurance....	(222.00)	
Banking......	(93.34)	
Total Cash Outflows		(2,032.87)
Cash at February 28, 2025		16,632.33

Notes:	Unrestricted cash	$12,025.97
	Restricted ARRL Grant	$2,962.31
	Restricted Pete Lawson Fund	$1,253.90
	Restricted IBM Grant	$390.15

NCRC Repeaters W1SYE and W1AAD


Antenna height 150 feet + or -
Transmit on RPT input freq 146.040mhz
Retransmits on RPT output freq 146.640mhz
10 Miles
10 Miles
Handheld
Repeater frequency 146.640mhz PL 107.2 offset .600-
Handheld

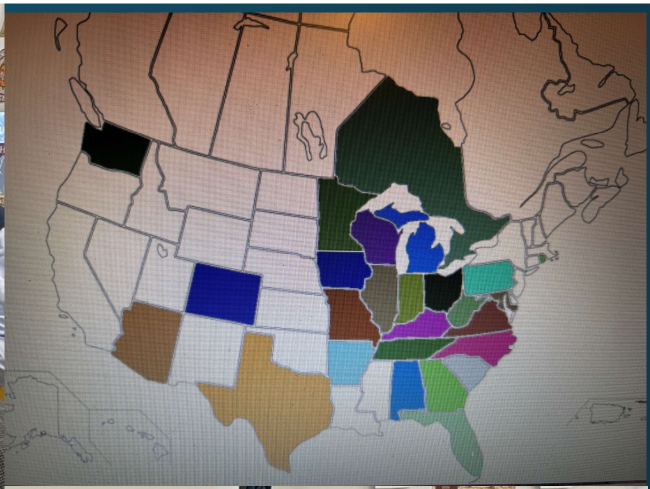
Dave Neal
W2DAN

Education & youth activities

School Club Roundup at All Saints Steam Academy February 10-14

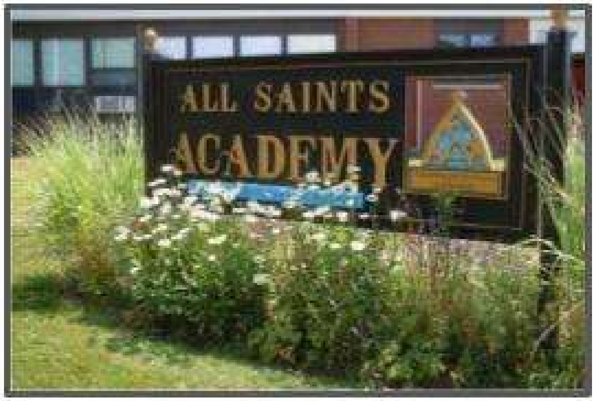
ALL SAINTS
STEAM ACADEMY
EAGLES
KAIZOU

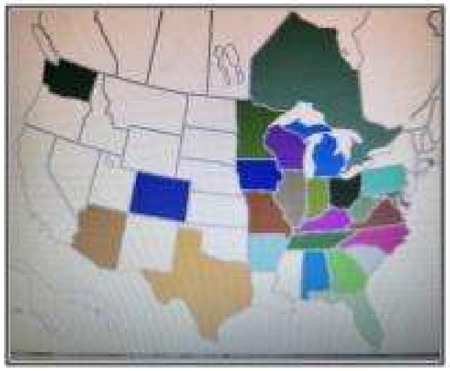
THE MAYA
ALL SAINTS
STEAM ACADEMY
EAGLES



ALL SAINTS
STEAM ACADEMY
EAGLES

ARRL SCHOOL CLUB ROUNDUP
@ ALL SAINTS STEAM ACADEMY
SETS RECORD 114 QSOS, 11,058 PTS
26 STATES, 13 SCHOOLS, 3 CLUBS





THANK YOU:

Jim KA1ZOU John KC1KOO
Rowan WO1P Mike K1NPT

Old Business

- Work on the Cube Smart 5x5 storage space in North Kingstown
- From the floor?

Our Cube Smart 5x5 storage space in North Kingstown

New Business

- Election of new Secretary.
- Poll of the membership to determine the extent of club equipment.
- Member service committee structure, work in progress.
- Updating the club trifold brochure.
- From the floor?
- Amendment of NCRC By-Laws, first reading.

Proposed Bylaw Changes

First Reading: March 14, 2025

Second Reading & Vote: April 14, 2025

Bob WB4SON

Why Change The Bylaws?

- Our club has grown dramatically in the past decade
- Situations have arisen not anticipated by the existing bylaws
- The existing bylaws are not always clear
- The club leadership needs to be able to respond flexibly and efficiently

Historically, the bylaws are revised every few years.

How The Bylaws Are Changed

- The Executive Committee, which takes care of club business, meets once or twice a month
- Areas needing to be modified are identified and discussed. Changes are gathered and eventually sent to the membership
- The proposed changes are presented to the membership for a “First Reading”, meant to announce the changes and prompt discussion
- After a second reading, the changes are voted on by the membership, and adopted following a simple majority vote of those present at the meeting

What Are We Changing?

- Rules for dealing with nominations for office
- Rules dealing with resignations
- Rules regarding special elections to replace officers
- Rules concerning meeting dates & locations
- Rules concerning the auditing of the club books
- A code of conduct for club members and users of club assets

Strikeout #1

- ARTICLE THREE – ADMINISTRATION
  - Section 1) The officers of the club shall consist of President, Vice President, Secretary, and Treasurer.
  - Section 2) The offices of President, Vice President, Secretary, and Treasurer shall be elective. Candidates for these offices shall be from the ranks of the active voting membership. They shall hold office for a period of one year. ~~The first business meeting of the new year shall mark the inauguration of the newly elected Officers unless such inauguration is impossible because of unforeseen circumstances. The outgoing officers shall hold office until the newly elected Officers are able to assume their duties.~~
  - Section 3) The resignation of any officer of the club may be accepted by the Secretary. If the office vacated is the President, the Vice President shall serve the remaining term as President, vacating the office of Vice President. ~~The President shall appoint a member to serve in the vacated position until a special election can be held at the next business meeting following notification of membership of the special election~~.

Details on handling resignations and replacements are now codified in ARTICLE EIGHT - NOMINATIONS AND ELECTIONS

Defining “Member At Large”

- ARTICLE ONE – OFFICERS
- Section 5) The Executive Committee shall consist of the President, Vice President, Immediate Past President, Secretary, Treasurer, and two to five Members At Large elected by the membership. The Executive Committee shall provide guidance and bring before the membership, issues and topics related to the well being of the Club and membership.

We never defined what those two to five members were called!

Revising Meeting Dates

- ARTICLE SIX – MEETINGS
- Section 1) The business meeting of the club shall be held on the second Monday of each month at 7:00 PM local time. When the second Monday falls on a holiday (October and November), the meeting shall be held on the third Monday. The Executive Committee, at its discretion may change the date of any meeting. A quorum of six Full Voting Members is required to conduct business.

As currently written, in theory every meeting HAD to be the second Monday. Now meeting dates can be changed

Audit Committee Report Due in MAY

- ARTICLE SEVEN – COMMITTEES
  - Section 1) The Executive Committee or President may establish standing committees and Chairpersons as needed.
  - Section 2) Special Committee Chairpersons shall be appointed by the President as required.
    - (a) Nominating Committee, a Chair plus two members who shall report no later than October 1st of each year, the names of Voting Members to be nominated for office at the November meeting and the offices for which they are to be nominated.
    - (b) Audit Committee of two members shall audit the Treasurer's books after the year-end financial report has been completed and present their findings no later than the May meeting.

The treasurer prepares monthly reports already. It was impossible to comply with a January deadline. A May date allows our volunteers to get together without undue pressure.

ARTICLE EIGHT - NOMINATIONS & ELECTIONS

- Section 1) The slate of officers proposed by the Nominating Committee shall be presented to the membership during the October meeting.
- Section 2) Nominations from the floor. Any member with voting privileges can be placed into nomination for any office of the club. Such a nomination must occur during the October meeting, must be moved and seconded and approved by a show of hands.
- Section 3) The election of officers will be held during the November meeting and will consist of the combined slate from the Nominating Committee and any floor nominations.
- Section 4) All positions that are not contested shall be elected by the Secretary (or designate) casting a single vote.
- Section 5) Any position that is contested shall be elected by a simple majority of votes placed by secret ballot of all members present during the November meeting. Should more than five Members At Large be on the ballot, the top five vote getters shall be elected.

ARTICLE EIGHT - NOMINATIONS & ELECTIONS

- Section 6) The secretary shall post a list of elected officers on the club website.
- Section 7) The period of time between the November meeting and the December meeting shall be used as a transition period
- Section 8) The formal transition of power to the incoming officers will happen on the second Monday in December (usually a year-end party).
- Section 9) The outgoing officers shall hold office until the newly elected Officers are able to assume their duties.
- Section 10) Should any officer resign, the President shall appoint a replacement. If the replacement comes from one of the elected Executive Committee members, then that person shall serve the remainder of the term (no special election is required). Members at Large do not need to be replaced until fewer than two remain. A special election is not required to be held in the last three months of the year.

Conduct clause added to ARTICLE NINE

- ARTICLE NINE – POLICY
  - Section 7) All members of the club are considered to be ambassadors of the club and are expected to extend good will to all members and non-members during on-air activities, in-person events, and club meetings. Users of club equipment, such as repeaters, are expected to keep their conversations congenial and not be disruptive or disrespectful to others.

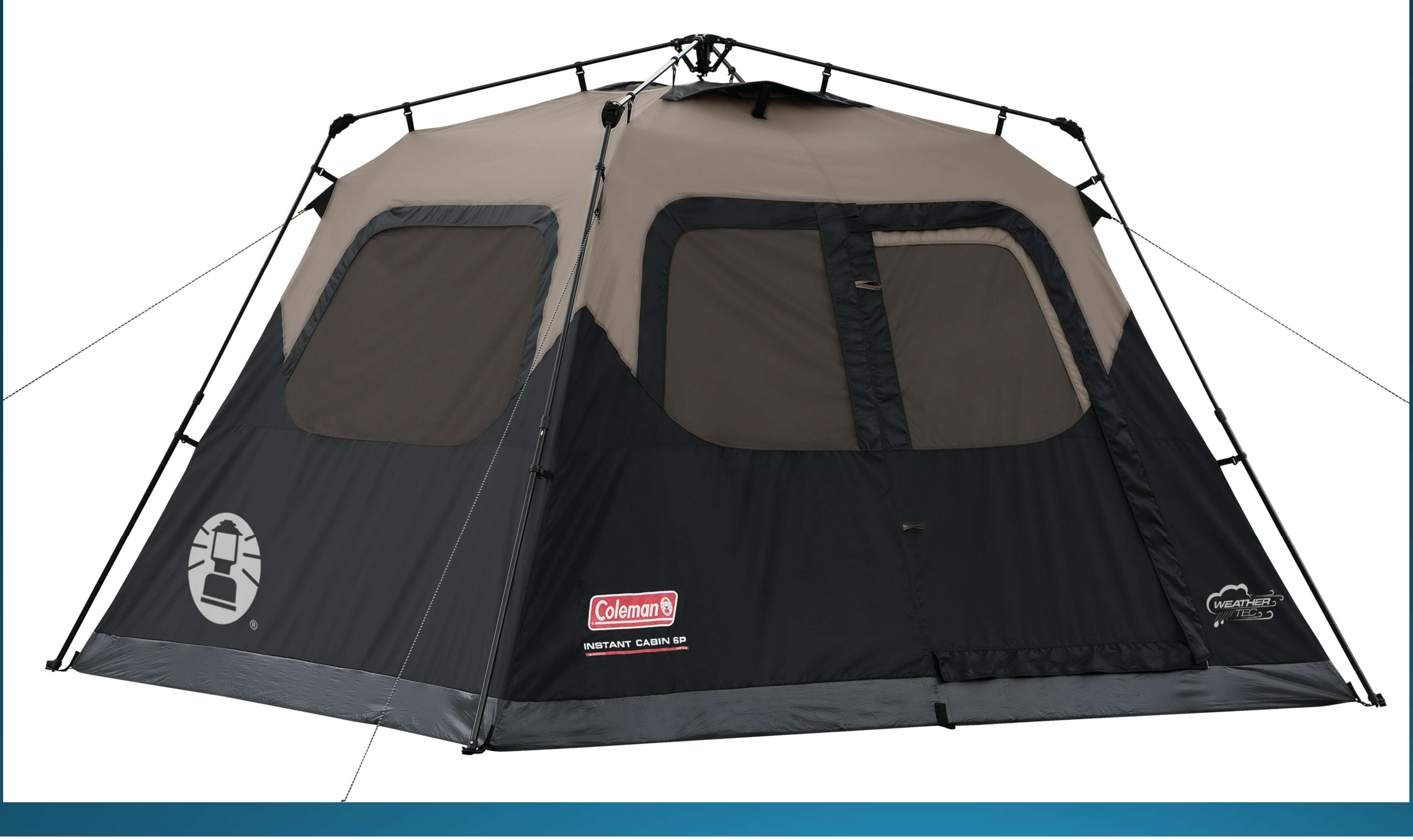
ARTICLE TEN -- TERMINATION

This concludes the first reading of amendments of the NCRC By-Laws

Executive Committee Highlights

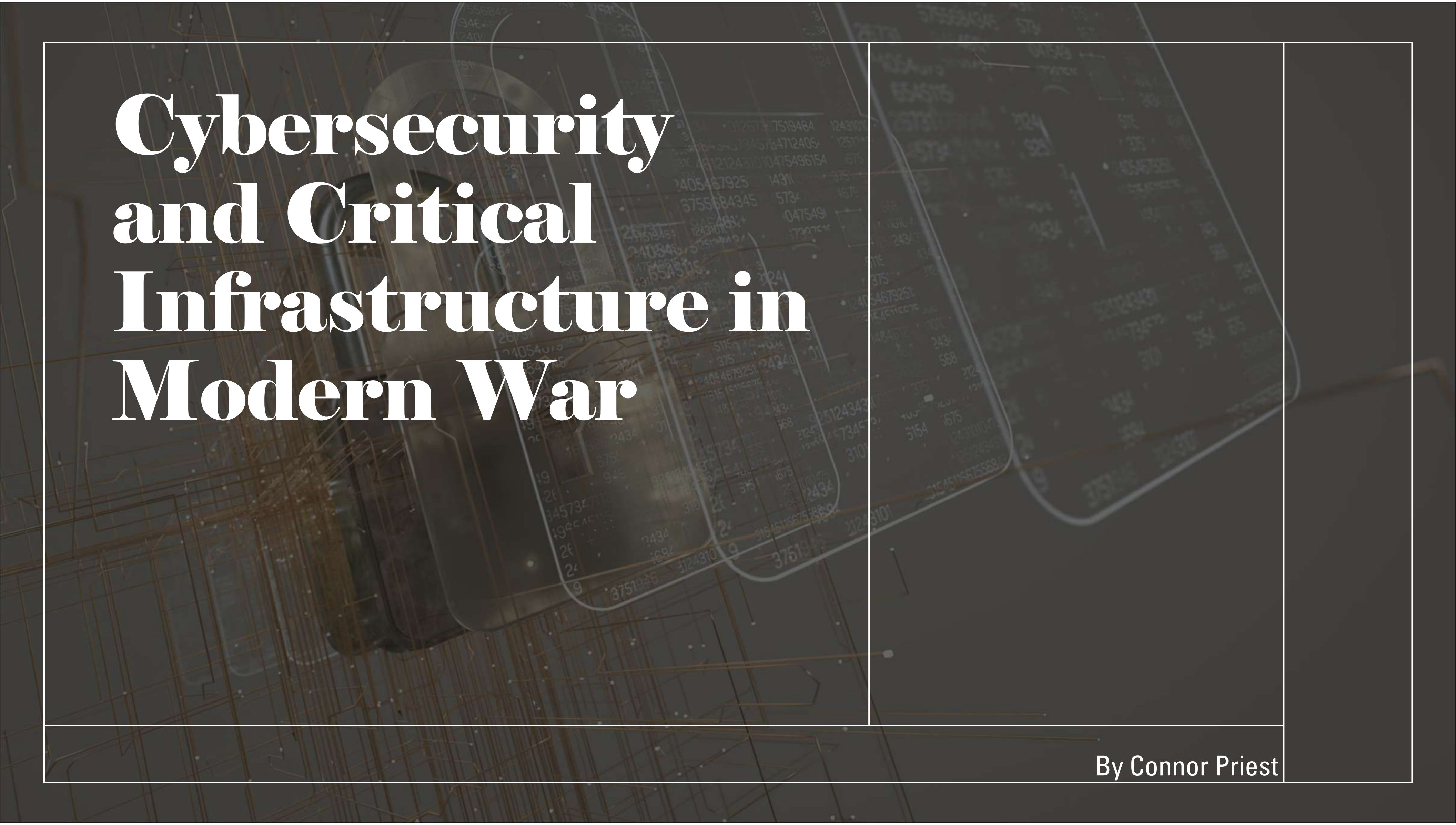
- Identification and reduction of club “stuff.”
- Organization and structure of club member services committees.
- Recruitment of members who would be willing to provide an informational service to others.

Coleman 6-person instant cabin



Breakfasts around and about are back. Old Mountain Lanes in Wakefild – more to come!

End
March Business Meeting



Cybersecurity and Critical Infrastructure in Modern War

By Connor Priest

Who am I?

- Connor Priest
- Senior at Roger Williams University
- Major: Cybersecurity and Networking
  - Minor: Computer Science
  - Minor: Digital Forensics
- Currently have an internship here at the War College working for the War Games Department.

Agenda

1. Cyber Terminology
2. Cyberwarfare and Military Operations
3. Critical Infrastructure Overview
    - 16 sectors
4. Incident 1 – Multi-Sector
5. Incident 2 – Hermetic Wiper
6. Incident 3 – Railway Attack
7. Incident 4 – Kyivstar
8. Final Thoughts/What Can You do?
9. Q/A

Cyber Terminology

- **Cyberwarfare**
  - Use of digital attacks by one country to disrupt, damage, or gain control over the information systems of another country.
- **Malware**
  - Malicious software designed to harm, exploit, or take control of a device. Types include viruses, worms, and ransomware.
- **Exploit**
  - A method or technique that attackers use to take advantage of a flaw or vulnerability in a system, often to gain unauthorized access.
- **Patch**
  - An update or fix released by software developers to correct a security vulnerability (exploit) or bug in the software.

Cyber Terminology

- **Ransomware**
  - Malware that encrypts a victim's files, demanding payment (often in cryptocurrency) to unlock or restore access to data.
- **DDoS Attack (Distributed Denial of Service)**
  - An attack where multiple systems overwhelm a server with requests, causing it to crash or become unavailable to legitimate users.
- **Zero-Day Vulnerability**
  - A security flaw that is unknown to the software maker and, thus, has no patch or fix, making it highly valuable to attackers.
- **IoT (Internet of Things)**
  - The interconnection via the internet of computing devices embedded in everyday objects, enabling them to send and receive data.

Cyberwarfare and Military Operations

- Cyberattacks have been more prevalent than ever, with attack numbers doubling almost every year (Microsoft).
- Proven to be capable of disrupting logistics, communication, energy, transportation
- The use of cyber in conjunction with kinetic attacks/troop movement has become much more prevalent and almost a standard where applicable, both defensively and offensively
- While modern military cyber-defense systems are typically secure in such a way that it is a deterrent to intruders, it is common to see attackers target surrounding systems/organizations where attacks would still have an impact on military operations
  - Examples include attacks disrupting public internet access, power, transportation, banking systems
  - If a defending nations people are at unrest or are uncomfortable, attackers gain an advantage

Critical Infrastructure at a Glance

- **Critical Infrastructure**
  - a network of systems, assets, and networks that are essential to the functioning of society
  - "considered so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof." (CISA*)
- While some forms of critical infrastructure are lesser affected by cyber-threats, the rapid digitization of all modern infrastructure can lead to the insecurity of a system that was once deemed safe.
- The specific sectors outlined in this presentation
  - Telecommunications, Gov. Services and Facilities, Transportation Services

*CISA - Cybersecurity & Infrastructure Security Agency

16 Critical Infrastructure Sectors

As Defined by the US Cybersecurity & Infrastructure Security Agency

- Chemical Sector
- Commercial Facilities Sector
- Communications Sector
- Critical Manufacturing Sector
- Dams Sector
- Defense Industrial Base Sector
- Emergency Services Sector
- Energy Sector
- Financial Services Sector
- Food and Agriculture Sector
- Government Services and Facilities Sector
- Healthcare and Public Health Sector
- Information Technology Sector
- Nuclear Reactors, Materials, and Waste Sector
- Transportation Systems Sector
- Water and Wastewater Sector

Cisa.gov

Multi-Sector

Incident

1

- NotPetya Cyberattack – June 2017
  - Major Sectors Affected: Energy, Transportation, Financial Services, Healthcare, Government, Food and Agriculture, Manufacturing
  - Victim: Ukraine (initial target), multinational effects
  - Attacker: Sandworm (Russian state-controlled hacker group)
  - Numbers Affected: 2,300+ organizations, 100+ countries
  - Timeframe: Weeks to Months
  - Impact: Primary goal of destroying systems and data
    - Estimated $10 Billion in total damages

Multi Sector Cont.

Incident

1

- Attack was carried out using a combination of two previously created malwares
  - EternalBlue – Exploit created by the NSA and leaked earlier that year
  - Mimikatz – PoC created by security researcher Benjamin Delpy in 2011
- The combination of the two allowed the virus to travel from one machine to the next, grabbing user passwords and login information, which allowed it to infect machines that were patched for the EternalBlue exploit
- Encrypted computers' master boot records*, making data irretrievable even if the ransom was paid

*Master boot record – part of the storage device that contains information needed to start the operating system

Multi Sector Cont. (Ukraine-Russia)

Incident
1

- Major government departments, including Ukraine's Ministry of Infrastructure, National Bank, and postal service, experienced severe disruptions. Many departments lost access to data and services crucial to national stability.
- Ukrainian banks, including major institutions like Oschadbank, had their networks compromised, disrupting ATM services and online banking for citizens.
- Key transportation hubs, including the Kyiv airport, experienced operational halts, leading to delays and grounding of flights, severely impacting both civilian and military logistics.
- Power distribution systems were affected, leaving some areas without electricity temporarily.
- A significant number of businesses, including hospitals, pharmacies, and retail stores, had systems crippled, leading to major supply chain issues and economic losses.

Gov. Services and Facilities

Incident

2

- Hermetic Wiper - Deployed February 23, 2022
  - Victims: Ukrainian Government (Ministry of Foreign Affairs, Ministry of Defense, Ministry of Internal Affairs, and the Security Service of Ukraine)
  - Suspected Attacker: Unknown Russian Threat Actors
  - Numbers Affected: Unknown
  - Timeframe: Less than a day
  - Primary Impact: Downtime for Hundreds of Ukrainian Gov. Linked Websites, destruction of data, and machine downtime

Incident

2

Gov. Services and Facilities Cont.

- Attack is very significant as the Hermetic Wiper malware was deployed only hours before the Russian invasion of Ukraine.
  - The capability of destroying government machines, communication systems, and the deletion of terabytes worth of data in coordination with a physical attack can cause massive disturbance.
- Attacks that target government networks also have the capability of hitting many sectors of critical infrastructure at once, as lateral movement within a network is easier once initial privileges are gained.
- Hermetic Wiper is still an active malware and has since been found on systems in Latvia and Lithuania.

Transportation Systems

Incident

3

- Polish Railway Attacks – August 25, 2023
  - Victim: Polish State Railways
  - Attacker: Unknown (16 arrested on allegation of spying for Russia)
  - Numbers Affected: Unknown
  - Timeframe: Aug. 25 – Aug. 28
  - Impact: 25+ passenger trains stopped, delay of transportation for hundreds of passengers, multiple freight trains halted, 1 derailment and 1 minor collision

Transportation Systems Cont.

Incident

3

- Attack was not a “modern” cyberattack and was carried out using only $30 worth of materials
  - Attackers used a radio spoofer and transmitted a series of tones to trigger the trains emergency stop functions
  - In some of the cases it was found that the remote stop signal was paired with a recording of the Russian National Anthem and a speech from Vladmir Putin
- Relevant to war in Ukraine as Poland serves as a major transport hub for western weapons being sent to Ukraine

Telecommunications

Incident

4

- Kyivstar Cyberattack - December 12, 2023
  - Victim: Kyivstar (Ukraine's largest telecom operator)
  - Suspected Attacker: Sandworm (Russian state-controlled hacker group)
  - Numbers Affected: 24 million+
  - Timeframe: Dec. 12 – Dec. 20
  - Primary Impact: Subscribers lost access to cellular network/internet. Thousands of virtual servers and personal machines wiped.
  - Secondary Impact: Disruption of some air raid sirens, banking systems, ATM’s and point of sale terminals that used Kyivstar chips

Telecommunications Cont.

Incident

4

- The methods of intrusion and type of malware used are still unknown
- It was believed that the hackers were within the telecoms system since at least May 2023, “hackers would have been able to steal personal information, understand the locations of phones, intercept SMS-messages and perhaps steal Telegram accounts with the level of access they gained”
  - 6-month period where attackers could quietly exfiltrate data

More Important Talking Points

- It is easy to show the direct impact and numbers of an attack that impairs public/private services, but data collection is something that cannot be quantized unless you are the hacker with the exfiltrated data
  - Many attacks that have happened against Ukraine such as HermeticWiper are also associated with data collection
- The SSSCIP* states that attackers have “gradually shifted to consolidating and covertly obtaining information and using the cyber component to obtain feedback on the results of their kinetic attacks”
  - This is due to countries like the US and companies such as Microsoft donating massive amounts recourses and time into Ukraine's cyber-defense systems

*SSSCIP - State Service of Special Communications and Information Protection of Ukraine

What can you do?

- It is likely that cyberattacks will not only continue but also become more prevalent and devastating as our world intertwines with the IoT (internet of things). The best thing for you to do is to stay informed and keep up with proper cyber practices.
- Update systems and devices regularly
  - Sometimes you wont even realize that there is an update unless you click the “check for update” button
  - Sometimes security updates are paired with content updates, so you might not realize that a specific update has anything to do with security unless you read the fine print
- Maintain a strong password policy, store them securely, use important ones sparingly.
- Stay vigilant online, don’t click random links/URLs, pay attention to login pages
- As annoying as it is, set up multi-factor authentication

Questions?

End of March meeting, 73

Unfortunately
Connor Priest
is unable to be with us